RAYANNE ALVES FELICIANO

A INCORPORAÇÃO DO PODER CIBERNÉTICO AO MILITAR: ANÁLISE ESTADUNIDENSE DO GOVERNO OBAMA

JOÃO PESSOA

2018

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

RAYANNE ALVES FELICIANO

A INCORPORAÇÃO DO PODER CIBERNÉTICO AO MILITAR: ANÁLISE ESTADUNIDENSE DO GOVERNO OBAMA

Monografia submetida ao curso de Relações Internacionais da Universidade Federal da Paraíba, como requisito obrigatório para obtenção do grau de Bacharelado.

Orientador: Prof. Dr. Augusto Wagner Menezes Teixeira Júnior

JOÃO PESSOA
2018

Catalogação na publicação
Seção de Catalogação e Classificação

F314i Feliciano, Rayanne Alves.
A incorporação do poder cibernético ao militar: análise estadunidense do governo Obama / Rayanne Alves Feliciano. - João Pessoa, 2018.
70 f. : il.

Orientação: Augusto Wagner Menezes Teixeira Júnior.
Monografia (Graduação) - UFPB/CCSA.

1. Ameaças cibernéticas. Espaço cibernético. 2. Estados Unidos. Poder cibernético. Poder militar. I. Teixeira Júnior, Augusto Wagner Menezes. II. Título.

UFPB/CCSA

RAYANNE ALVES FELICIANO

A INCORPORAÇÃO DO PODER CIBERNÉTICO AO MILITAR: ANÁLISE ESTADUNIDENSE DO GOVERNO OBAMA

Monografia apresentada ao Curso de Relações Internacionais da Universidade Federal da Paraíba, como requisito parcial à obtenção do título de bacharel (a) em Relações Internacionais

Aprovado (a) em 9 / 11 / 2018

BANCA EXAMINADORA

Prof. Dr. Augusto Wagner Menezes Teixeira Junior (Orientador)
Universidade Federal da Paraíba - UFPB

Prof. Dr. Gills Vilar Lopes
Universidade Federal de Rondônia - UNIR

Prof. Dr. Fábio Rodrigo Ferreira Nobre
Universidade Estadual da Paraíba - UEPB

RESUMO

A emergência do espaço cibernético e dos riscos associados a ele demonstram que se um país quiser deter poder internacional, garantir sua sobrevivência, segurança e interesses, necessariamente precisa desenvolver o poder cibernético. Buscando não apenas vencer as ameaças do espaço cibernético, mas também acessar as vantagens desse meio, os Estados buscam desenvolver o poder cibernético atrelando-o à sua estratégia de segurança e defesa nacional. Este trabalho se preocupa especificamente em entender como os Estados Unidos da América (EUA) incorporam o poder cibernético ao militar, tendo como recorte temporário os dois governos Obama. Por meio de uma pesquisa qualitativa descritiva exploratória, baseada na teoria realista das Relações Internacionais e analisando os documentos da *National Security Strategy* de 2010 e 2015 e as estratégias para o espaço cibernético do Departamento de Defesa americano de 2011 e de 2015, perceberam-se esforços dos EUA em transformar o espaço cibernético em um domínio, ou seja, em garantir que as Forças militares convencionais tenham capacidade de atuação também nele. Contudo nota-se que, embora interligada às demais expressões do poder militar, a estratégia de poder cibernético não é pensada com o objetivo único de complementar as vertentes convencionais do poder militar, tampouco essa estratégia de incorporação do poder cibernético é articulada necessariamente às outras Forças; há sim, uma preponderância nos documentos para a visão de que, como um domínio independente, o espaço cibernético requer investimentos exclusivos e uma Força também exclusiva, razão pela qual o país criou a Cyber National Mission Force. Logo, o poder cibernético é incorporado de modo independente das demais Forças dentro do poder militar dos Estados Unidos.

Palavras-chave: Ameaças cibernéticas. Espaço cibernético. Estados Unidos. Poder cibernético. Poder militar.

ABSTRACT

The emergence of cyber space and the risks associated with it demonstrate that if a country wants to retain international power, ensure its survival, security and interests, it must necessarily develop cyber power. By linking it to the military power through the strategy of national security and defense, States are be able to overcome the threats of cyberspace, and to access its advantages. This work is specifically concerned with understanding how the United States of America is incorporating cybernetic power into the military, with the Obama Administration as a temporary cut. Through a descriptive qualitative exploratory research based on the realistic theory of International Relations and observing the National Security Strategy documents of 2010 and 2015 and the US Department of Defense's strategies for cyberspace in 2011 and 2015, it was perceived the US efforts to transform cyberspace into a domain to ensure that the conventional military forces are also capable of acting in it. Nevertheless, it is noteworthy that, although interlinked with other expressions of military power, the strategy for the development of cybernetic power is not being thought with the sole objective of complementing the conventional aspects of military power, nor is this strategy of incorporation cyberpower necessarily articulated to the other Forces, there is a preponderance in the documents for the view that as an independent domain, cyber space requires exclusive investments and a Force also exclusive, which is why the country created the Cyber National Mission Force. Therefore cyberpower is incorporated independently of the other Forces within the military power of the United States.

Key words: Cyberpower. Cyberspace. Cyber threats. Military power. The United States.

SUMÁRIO

1 INTRODUÇÃO

O poder é essencial aos Estados para que eles possam garantir sua sobrevivência e seus objetivos políticos. Ao longo dos séculos, o poder militar[1] é capaz de conferir aos países capacidade de exercer influência nos mais diversos domínios. A terra e os mares são espaços em que, desde as civilizações mais remotas na Mesopotâmia, China e Egito, há a preocupação em se desenvolver força militar com a intenção de dominar tais ambientes. Com o passar dos anos, conforme avanço das tecnologias, outros domínios ganham importância, e os Estados passam a contabilizá-los em suas estratégias de defesa.

A partir do século XX, o domínio dos meios aéreo e espacial por meio dos poderes aéreo e nuclear foi fundamental não só para a vitória, como também para a manutenção no sistema internacional dos países vencedores das duas Grandes Guerras. No pós-Segunda Guerra Mundial, com a consolidação dos Estados Unidos da América (EUA) e da União Soviética como potências mundiais e a consequente polarização do mundo, o poder nuclear determinou-se como um fator distintivo entre potências mundiais e demais Estados, além de se tornar fator de garantia de sobrevivência e de maior probabilidade de atingir os interesses próprios.

Se, no século XX, os poderes aéreo e espacial passaram a ser considerados como de extrema necessidade para defesa estatal e projeção de poder, no século atual, a ascensão do espaço cibernético como lugar significativo de parte das atividades humanas e estatais coloca como urgente e imprescindível o desenvolvimento de um novo tipo de poder, o cibernético (NYE,2010) . Desde a revolução informacional no final da década de 1990, ocorrida a partir do advento da informática e da Internet, junto ao processo de intensificação da globalização, as tecnologias de informação e de comunicação (TIC) estão tornando-se cada vez mais elaboradas e difundidas, impactando não só cidadãos como também atores estatais.

O espaço cibernético é mais um domínio em que a anarquia característica do sistema internacional se apresenta. Com isso, há um aumento da noção de insegurança nos Estados, o que os leva a adotar estratégias para garantir sua segurança, visto que inexiste um governo comum aos Estados regulando o comportamento geral dentro do espaço cibernético e que a

[1] Neste trabalho, poder militar é entendido como umas das expressões do poder nacional, composto também pelo poder diplomático e econômico. Compreende-se que fazem parte do poder militar os poderes terrestre, aéreo e naval, vertentes de poder que conferem ação nos diferentes domínios. Essas compreenssões serão melhor exploradas na próxima seção.

ocorrência de ataques cibernéticos cria um desbalanceamento no poder internacional, podendo aumentar os riscos de conflito.

Surge assim nos Estados a necessidade de garantir sua presença no espaço cibernético, para construir uma resiliência contra possíveis ataques cibernéticos, o que se torna possível com a aquisição de poder cibernético, isto é, "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power " (KUEHL, 2009, p. 38).

Desde o início dos anos 2000, os EUA estão investindo na defesa do espaço cibernético e, portanto, direcionando esforços no sentido de incorporar o poder cibernético na segurança e na defesa nacional. Contudo, em 2008, uma comissão organizada pelo Centro para Estudos Estratégicos e Internacionais (CSIS), em Washington, produziu um relatório cuja conclusão apontou que "America's failure to protect cyberspace is one of the most urgent national security problems" (CSIS, 2008 *apud* GADY; AUSTIN, 2010, p.1; OBAMA, 2009) fazendo crescer naquele país a percepção de vulnerabilidade no espaço cibernético.

Como resposta ao aumento dessa percepção de insegurança, o presidente Obama lançou uma nova política de cibersegurança em 2009, expressando sobre a defesa cibernética norte-americana: "we're not as prepared as we should be [...] we've failed to invest in the security of our digital infrastructure." (AMERICA, 2009 *apud* GADY; AUSTIN, 2010, p.1)

Falhas na segurança do espaço cibernético[2] são problemáticas principalmente porque é um domínio que ainda carece de regulações e coloca grandes desafios de segurança para os Estados. O meio de superar esses desafios é pelo desenvolvimento do poder cibernético. Voltando-se para os Estados Unidos no governo Obama (2009-2016), têm-se por problema de partida: Como os Estados Unidos estão incorporando o poder cibernético ao poder militar? Neste sentido, o objetivo deste trabalho é evidenciar a ampliação do poder militar dos Estados Unidos ao incorporar o poder cibernético à sua estratégia de defesa nacional.

Nota-se, assim, que o estudo proposto aqui é voltado, em essência, para a discussão sobre o poder nacional, especificamente o poder militar ampliado com o poder cibernético em

[2] Falhas na segurança do espaço cibernético expõem as vulnerabilidades de infraestruturas críticas dos Estados como redes elétricas, de transporte e de comunicação que dependem do espaço cibernético para funcionar. Com isso, os sistemas que controlam essas redes correm o risco de sofrer ataques cibernéticos, os quais podem causar desde a indisponibilidade dos serviços até a destruição das redes.

razão do surgimento de uma nova fonte de ameaça, o espaço cibernético. A discussão é sobre as capacidades de um Estado exercer influência, atingir seus objetivos e principalmente garantir sua sobrevivência no contexto dos novos desafios colocados pelos avanços tecnológicos. O propósito deste trabalho está relacionado ao emprego do poder cibernético no sentido defensivo, isto é, no exercício do poder cibernético militar com o objetivo último de garantir a sobrevivência do Estado.

A hipótese é de que essa incorporação ocorre de modo complementar às estratégias militares convencionais, não sendo aplicada ou pensada na estratégia dos EUA a efetivação do poder cibernético para a defesa nacional de modo desassociado das demais Forças.

Com a evolução da tecnologia de informação do século XXI, o espaço cibernético constitui-se não só como um meio de comunicação rápida, mas também como mais um meio estratégico de poder, sendo mais um importante ambiente de ataque e de defesa dos Estados forçando-os a visualizarem o domínio do setor cibernético e sua inclusão às estratégias militares de segurança nacional como medidas necessárias.

Logo, estudar o poder cibernético e realizar um estudo direcionado a um país com um histórico significativo de poder bélico torna-se importante na medida em que se busca, para além de constatar a securitização do espaço cibernético empreendida pelos Estados Unidos, identificar o modo como o desenvolvimento do poder cibernético está sendo incorporado à estratégia militar e consequentemente tornando o país mais forte nas relações internacionais.

O presente trabalho configura-se como uma pesquisa qualitativa descritiva exploratória, fazendo uso da literatura sobre relações internacionais, poder cibernético e defesa cibernética, além de documentos oficiais públicos de defesa dos Estados Unidos. Assim, propõe-se a mostrar como a incorporação do poder cibernético é possível de ser realizada no nível da defesa militar.

Para tanto, este trabalho está dividido em três seções principais. A primeira, com abordagem mais teórica dentro das Relações Internacionais (RIs), visa explorar o entendimento do poder, tendo por base a escola teórica realista, tendo-se em consideração o fato de que a discussão sobre poder possui elevada importância para essa escola, mas também considerando o fato de que, principalmente desde a segunda metade do século XX até os dias atuais, o Realismo exerce forte influência nas políticas dos EUA. Desse modo, apresentar-se-á o poder como necessidade para os Estados dentro de um ambiente anárquico e a emergência

do poder cibernético, respondendo aos anseios dos países de manter sua segurança frente ao novo domínio, o espaço cibernético.

Entendido o poder e compreendida a necessidade estatal de desenvolver o poder cibernético, na segunda seção, este poder será explorado, definindo-se os aspectos de vulnerabilidade e vantagem do espaço cibernético que o fazem emergir, mostrando assim a relação entre o poder cibernético e a segurança nacional.

Finalmente, a última seção realiza um estudo da estratégia[3] americana de defesa do governo Obama, a fim de perceber como os EUA buscaram incorporar o poder cibernético ao militar, aumentando, com isso, a capacidade de sobrevivência do Estado no ambiente internacional.

[3] Os Estudos Estratégicos exploram as causas, as consequências e especialmente a conduta da guerra, isto é, as opções de como fazer a guerra (PROENÇA; DUARTE, 2007). Quando este trabalho volta-se para o estudo da estratégia americana para o espaço cibernético, busca, portanto, perceber como esse meio é articulado nos Estados Unidos enquanto espaço de guerra.

2 O PODER NA TEORIA REALISTA DE RELAÇÕES INTERNACIONAIS

Na visão realista das relações internacionais, o ambiente anárquico em que estão inseridos os Estados torna imperativa a necessidade de defesa nacional, e, para tanto, o desenvolvimento do poder. Nesta perspectiva, esta seção tem por objetivos: 1) introduzir as noções de poder nas RIs, tendo-se por base, a escola teórica realista; e 2) identificar a emergência do poder cibernético, conforme o avanço tecnológico do final do século XX tenha trazido a percepção de um novo domínio em que a ameaça a sobrevivência nacional pode concretizar-se, o espaço cibernético.

Desse modo, inicialmente será tratada a escola realista e sua percepção do poder como necessidade e como interesse de um Estado gerando as concepções de política de poder e política de força. Em seguida, será definido o conceito de poder, esclarecidas as fontes que o geram e as formas como ele se concretiza, para, em última instância, ser apontada a ampliação do poder nacional com a incorporação do poder cibernético.

2.1 O PODER COMO NECESSIDADE E OBJETIVO DOS ESTADOS SOBERANOS

A escola realista é a corrente de pensamento mais antiga das RI, motivo pelo qual diferenciam-se o realismo clássico e o neorrealismo. Embora existam essas nomenclaturas da escola realista, alguns princípios podem ser-lhe considerados comuns. Em primeiro lugar, a centralidade do Estado e seu principal objetivo de garantir a sobrevivência, no sentido de que o Estado, como ator principal das relações internacionais tem como valores fundamentais a segurança nacional e a sua própria sobrevivência, pela conservação de seu poder e preservação da ordem (CASTRO, 2012). Em segundo lugar, a busca pelo poder como um fim em si mesmo ou um meio para outros fins. E em terceiro lugar, a estrutura da anarquia internacional, isto é, "a falta de um governo central, supranacional, capaz de correlacionar, eficazmente, as normas e instituições internacionais" (CASTRO, 2012, p. 318), cujo resultado é a autoajuda, ou seja, cada Estado utiliza de suas próprias capacidades para defender seus interesses e sobreviver (WALTZ, 1983).

Percebe-se, assim, que as noções de Estado, anarquia, sobrevivência e poder são fundamentais no Realismo. Pela leitura dos autores desta escola teórica, é possível perceber, principalmente em Kenneth Waltz, a referência ao poder tanto como uma necessidade de todo Estado, quanto como o objetivo imediato de toda ação política estatal, destacando-se Hans Morgenthau. A seguir, serão exploradas essas duas concepções do poder dentro do Realismo: como uma necessidade e como objetivo.

Tratando-se inicialmente do poder como uma necessidade, é preciso ter clara a noção de anarquia internacional, apontada como um princípio marcante do pensamento realista nas RI. O neorrealista Waltz (1983) definiu a anarquia como um espaço em que a ameaça da violência e o recorrente uso da força são característicos, mas que, além disso e principalmente, é um espaço distinguido pelo fato de que o uso desta ocorre em uma estrutura desprovida de um governo, isto é, na ausência de uma instituição que detenha o uso legítimo da força.

Entendendo a anarquia, torna-se mais fácil compreender o poder como uma necessidade. Dentro desse cenário internacional anárquico, a condição predominante é de insegurança, impondo aos Estados o "medo hobbesiano", em que uma potência não tem a garantia de que uma outra não é inimiga (WIGHT, 2002). Sem propensão a abdicar de sua soberania e entregar a uma instituição global a sua segurança pessoal, a norma para os Estados, dentro do contexto de desconfiança mútua, é nos dizeres de Hobbes (1983), ter as armas e os olhos voltados uns para os outros, podendo fazer o que for necessário para garantir sua preservação (WALTZ, 1983). Porquanto os Estados não possuem garantia de sobrevivência no ambiente de anarquia, torna-se imprescindível a detenção de poder, assim, pode-se afirmar que, no Realismo, o poder é uma necessidade.

Ao mesmo tempo, o poder dentro do Realismo também pode ser visto como um objetivo dos Estados. A percepção da elevada importância do poder para as nações, assumindo caráter de objetivo imediato das ações políticas estatais é inerente à teoria realista das RI, sendo afirmada no segundo princípio básico do realismo erguido por Morgenthau (2003, p.48), qual seja: “o conceito de interesse [dos Estados é] definido em termos de poder” (MORGENTHAU, 2003, p. 48). Para essa perspectiva teórica, tal conceito é central pois: 1) encerra em si mesma a razão de toda ação política internacional — isto é, a busca pelo poder — e 2) apresenta a característica que distingue um fato político de um não-político ao fornecer a compreensão de que toda política é uma luta pelo poder e que independentemente

de qual seja o fim ambicionado por ela, o poder é sempre seu objetivo imediato. Esclarece, Morgenthau (2003), no terceiro princípio do Realismo, que o tipo de interesse e de poder perseguidos pela ação política não são fixos e permanentes, mas, sim, determinados pelo contexto cultural e político, no sentido de que os objetivos de uma nação são modificados ao longo do tempo, bem como o conteúdo e a maneira de utilizar o poder também sofrem alterações conforme desenvolvam formas mais eficazes de estabelecer e manter controle sobre as pessoas.

No entanto, Morgenthau (2003) defende que toda atividade política sempre pretende realizar um destes três objetivos: conservar, aumentar ou demonstrar o poder. Desse modo, pode-se inferir que no decorrer da história humana, as nações, conforme o contexto, terão interesses distintos em termos de poder, todavia, essa modificação será quanto a conservar, aumentar ou demonstrar seu poder, o que quanto ao tipo de política tomada pelo Estado será respectivamente: manutenção do *status quo*, ampliação das relações de poder existentes ou busca por prestígio. Esses três interesses ou objetivos dos Estados intimamente relacionados ao poder demonstram o segundo aspecto do poder dentro da teoria realista, a saber: o poder como objetivo.

2.1.1 A política, o poder e a política do poder

Uma vez entendido, do ponto de vista realista, a concepção do poder como necessidade, sobrevivência e segurança, e como objetivo, interesse de manter o *status quo,* ampliar poder ou demonstrá-lo, pode-se compreender a política internacional como uma luta pelo poder.

Para a compreensão da chamada “ política do poder ”, serão trazidas considerações de Martin Wight, que, embora representante da Escola Inglesa de sociedade internacional, por defender que há três grandes paradigmas no comportamento dos Estados — realismo, racionalismo e revolucionarismo — possui em seus escritos elementos da escola realista. Desse modo, as reflexões de Wight sobre a “política do poder” são de grande valia para o presente trabalho.

Tal termo implica duas condições: em primeiro lugar, a de que há “unidades políticas independentes que não reconhecem superior político e que se consideram ‘soberanas’ ”, isto é,

os Estados; e em segundo lugar, a de que “existem relações contínuas e organizadas entre elas” (WIGHT, 2002, p.1), ou seja, há relações políticas, econômicas, diplomáticas, comerciais, de paz e de guerra.

Como este trabalho tem por objetivo analisar o uso do poder militar — força — por parte do Estado atrelado ao poder cibernético, é bastante útil para os propósitos deste trabalho a consideração de Wight (2002) de que a origem do termo “política do poder”, mais precisamente, a palavra alemã *Machtpolitik,* que significa “política da força, ou seja, a condução de relações internacionais por intermédio da força ou da ameaça do uso da força” (WIGHT, 2002, p. 8).

Decorre, dessa afirmação, que a política do poder entre Estados soberanos evidencia um dos principais elementos do poder de acordo com a teoria realista: o de uso da força e o de ameaça do uso da força — poder militar —, servindo a defesa dos interesses nacionais. O uso da força na visão realista serve ao propósito de limitar manipulações, moderar demandas e resolver conflitos (WALTZ, 1983). O uso da força como exercício de poder do Estado é o uso do poder militar, o qual pode ser utilizado de modo isolado ou em conjunto com as outras formas de poder nacional quando o Estado visa alcançar seus objetivos.

Antes de tratar da temática sobre poder nacional e exercício de poder, julga-se necessária a explicação sobre o que constitui o poder dos Estados, ou seja, qual a natureza do poder. Assim, a seguir o poder será definido e, na sequência, será retomada a discussão sobre o exercício de poder pelo Estado, para, enfim, relacioná-lo ao poder cibernético.

2.2 O PODER DO ESTADO

O poder é um elemento essencial da política e indispensável a um governo. Seja o Estado uma grande potência, ou seja uma pequena e fraca nação, ele estará preocupado com a sua força e interessado em aumentá-la e projetá-la, pois a expressão da política como “política de poder” ou como “política de força” aplica-se a qualquer país que objetiva garantir sua capacidade de governar e sua segurança nas relações internacionais. (CARR, 2001)

Sabendo-se do caráter indispensável do poder na política internacional e em especial, dentro da teoria realista, cabe o seguinte questionamento: o que é poder? Há várias definições de poder nas RI e pouca concordância sobre como conceituar o termo estudá-lo ou medi-lo

(BALDWIN, 2016). Uma das definições é a de Dahl (1975), para quem o poder é a capacidade de fazer com que outros façam o que em outras circunstâncias não fariam .

Autores realistas, como Waltz e Morgenthau, afirmam que o poder está relacionado à capacidade de controle. Os Estados como detentores de poder político controlam uns aos outros, o que significa dizer que eles conseguem gerar resultados que não ocorreriam naturalmente (CHIAPPIN, 2010; MORGENTHAU, 2003)

Dentro do espaço anárquico em que ocorrem as relações interestatais, o que torna um Estado forte ou com grande poder no ambiente internacional não provém do impacto de um exercício legal, de um direito de dominar: "*the power of the strong may deter the weak from asserting their claims, not because the weak recognize a kind of rightfulness of rule on the part of the strong, but simply because it is not sensible to tangle with them*." (WALTZ, 1983, p. 113).

Neste contexto, o que permite a um Estado gerar impacto na mente de outros atores, a ponto de que estes não sejam sensíveis a entrar em disputa com aqueles? Precisamente será o grau de poder que tal Estado conseguir exercer e demonstrar, fazendo-o ser considerado uma potência militar no sistema internacional.

2.3 O EXERCÍCIO DO PODER NACIONAL

O exercício do poder nacional garante ao Estado a possibilidade de que ele, no meio internacional, consiga deter outras potências e possa conservar, aumentar ou manter seu poder. Este trabalho discute as ações estatais consideradas como exercício do poder político as quais podem ser evidenciadas enquanto: a) poder diplomático; b) poder econômico; e, c) poder militar. Apesar de que "the economic, military and other capabilities of nations cannot be sectored and separately weighed" (WALTZ, 1983, p. 131), para fins deste estudo, ele pode ser subdividido em categorias interdependentes (CARR, 2001).

Na prática, o uso de um ou outro poder como meio para um Estado alcançar seus interesses realizar-se-á conforme o governo entenda que o exercício de poder escolhido - diplomático, econômico ou militar - é suficiente para produzir os resultados desejados na ação dos demais Estados. Retomando a discussão do subitem 2.1.1, a "política do poder" normalmente será identificada pelo exercício do poder diplomático e econômico, enquanto a

“política da força” ocorre pela concretização do poder militar. Cada uma poderá ser aplicada isoladamente ou em combinação de acordo com o entendimento de qual política será a mais eficaz.

No tocante às estratégias de defesa, o poder militar é o principal. Quanto maior a percepção por outros países que um país “A” detém poder militar elevado, menor será a motivação deles para engajar-se em um confronto físico ou não concordar com o posicionamento daquela potência militar. O país com destaque no campo militar ganha capacidade retaliatória e prestígio que quando grandes o suficiente, atrelam seu poder militar à dissuasão e, assim, sua defesa nacional torna-se mais eficaz e menos dependente do uso concreto da força, sendo bastante apenas a ameaça de uso da força.

Os outros exercícios de poder somam-se ao militar, tornando o país mais forte e mesmo impedindo que a percepção de insegurança no ambiente anárquico evolua para um confronto físico com o emprego efetivo da capacidade militar. Nesta perspectiva, os poderes diplomático e econômico contribuem para a estratégia de defesa nacional no sentido de evitar a ocorrência de guerra.

Na sequência, serão explicitas outras peculiaridades do exercício dos poderes: diplomático, econômico e militar.

2.3.1 Poder diplomático

Este tipo de poder é entendido como a capacidade de controle do Estado sobre o meio diplomático das relações internacionais, fazendo uso dos fatores intangíveis de influência.

O poder diplomático, durante a paz, condiz ao que o poder militar representa durante a guerra: (MORGENTHAU, 2003). Esse poder constitui a possibilidade de os Estados, por meio da negociação e da barganha, produzir efeitos desejados em outros atores estatais em tempos de paz. (MINGST, 2009). O poder nacional, expresso nessas negociações e barganhas, deriva também da visão de que o Estado possui sobre suas “vantagens de localização geográfica, de autossuficiência em alimentos, matérias-primas e produção industrial, do grau de preparo militar e do tamanho e qualidade da população” (MORGENTHAU, 2003, p. 274).

Se o país detentor dessas fontes potenciais de poder não possuir uma diplomacia igualmente robusta, com perspicácia para alcançar o máximo de proveito que essas fontes permitem, ele cederá a um outro Estado, diplomaticamente mais forte. Desse modo, o poder diplomático torna-se de grande importância para que o Estado atinja seus interesses.

2.3.2 Poder econômico

O poder econômico refere-se à capacidade que o Estado possui de controlar resultados na esfera econômica de suas relações. Sobre esse poder, é possível afirmar que ele importa por dois motivos: o primeiro é a autarquia, ou autossuficiência, trazendo a inferência de que quanto mais bens manufaturados uma nação consegue produzir, tanto mais atenderá às demandas sociais, e tanto mais bem preparada estará para a guerra, uma vez que terá pouca dependência de importações de bens essenciais (CARR, 2011).

O segundo motivo provém da possibilidade de empregar medidas econômicas para influenciar outros países, principalmente por meio de sanções. Neste caso, quando um Estado controla elevadas quantidades de um recurso escasso e essencial, mais poder ele tem nas relações internacionais (MINGST, 2009).

2.3.3 Poder militar

O poder militar tem elevada importância, porquanto “todo ato do Estado, no aspecto do poder está dirigido para a guerra, não como uma arma desejável, mas como uma arma que pode ser necessária como último recurso ” (CARR, 2011, p. 143).

A guerra é um “ato de violência destinado a forçar o adversário a submeter-se à nossa vontade” é, pois, um “meio sério para alcançar um fim sério” (CLAUSEWITZ, 2003, p.7). Esse meio sério corresponde à força militar empregada em contexto de guerra, enquanto o fim é o interesse político. Nesse sentido, há aqui a retomada da discussão iniciada na subseção 2.1.1 delineando-se mais clara a expressão “política da força”, pois a força é utilizada com objetivo político. E em outras palavras, a política — isto é, as ações de um Estado — traduz-se no uso da força quando ele julga necessário tal recurso para alcançar um interesse.

O poder militar atenderá aos dois aspectos do poder identificados na teoria realista, a saber, o poder como necessidade e como objetivo. O poder militar tanto poderá ser utilizado para desarmar o inimigo e garantir a sobrevivência e segurança estatal — necessidade —, quanto poderá ser utilizado para o alcance do objetivo político de poder nas relações externas, uma vez que o uso da capacidade militar permite a um país evitar insubordinação de outros atores e consequentemente afirmar seu poder e, até mesmo, aumentá-lo.

Geoestrategicamente, são três os poderes militares tradicionais de uma nação: marítimo, terrestre e aéreo discutidos a seguir.

2.3.3.1 Poder marítimo

O domínio do mar pela força militar marítima contribuiu para o aumento das capacidades estatais, ao tornar a artilharia móvel: “numa época em que os canhões em terra tinham de ser penosamente arrastados, navios carregavam os seus pelo mundo afora” (WIGHT, 2002, p. 53).

Até aproximadamente 1945, predominou na política internacional o poderio marítimo (WIGHT, 2002), o que, na concepção do teórico do poder marítimo, Alfred Mahan, atesta a superioridade do controle sobre o mar nas lutas comerciais e militares. Uma das razões da primazia da força naval seria a capacidade de ultrapassar obstáculos geográficos que o poder terrestre não consegue, (CASTRO, 1999), e, além disso, a capacidade de agressão gerada pelo mar, isto é, possibilidade de apoiar aliados e pressionar inimigos, como força dissuasória, ao ameaçar usar o poder marítimo em pontos terrestres estratégicos e assim neutralizar e debilitar adversários (MAHAN *apud* CASTRO, 1999; BULL, 2002). Um exemplo concreto do poder naval assim aplicado são os bloqueios navais da costa inimiga.

2.3.3.2 Poder terrestre

O fim do século XIX foi marcado pelo avanço tecnológico e pelas grandes invenções, dentre as quais destaca-se a locomotiva. A rápida construção de ferrovias transcontinentais, permitindo o encurtamento de distâncias e a interiorização do continente eurasiano, levou Mackinder a entender que se iniciava ali uma nova era na qual a importância do barco a vapor

e do poder marítimo cederiam lugar para o poder terrestre (WIGHT, 2002). Em sua teoria do poder terrestre, o Heartland — região continental central da Eurásia — é vista como o domínio fundamental na política de poder das grandes potências:

> Segundo Mackinder, a exploração dos inesgotáveis recursos da região basilar da Eurásia daria ao Estado que a controlasse condições para desenvolver um inexpugnável poder terrestre. [...] Se o Estado-pivô conseguisse apossar-se de uma vasta frente oceânica poderia canalizar os recursos do Heartland para a edificação de um poder marítimo. A ascensão de um poder anfíbio, sem igual no continente eurasiático e capaz de rivalizar com a Inglaterra nos oceanos, acabaria por suplantar o poder marítimo inglês na luta pela preponderância mundial (MELLO, 1994, p.59).

Como é perceptível no trecho acima, para Mackinder, uma razão da superioridade do poder terrestre é decorrente da possibilidade que essa força tem de lançar-se ao mar e fazer ações bem sucedidas, defendendo que é mais fácil ao poder terrestre formar uma esquadra que ao poder marítimo organizar um exército. Evocando episódios históricos, ele sustenta sua argumentação, identificando momentos em que Estados com amplo poder terrestre conseguiram construir uma frota naval forte o suficiente para derrotar inimigos — a exemplo de Esparta, na Guerra do Peloponeso — e circunstâncias em que potências marítimas foram derrotadas pela força terrestre de seus adversários — como em Alexandre e o domínio da frota persa de Tiro — (WIGHT, 2002, p.58).

2.3.3.3 Poder aéreo

Do mesmo modo que o avanço tecnológico — por meio de navios, locomotivas — permitiu a percepção de superioridade dos poderes naval e terrestre, o avião foi o progresso que no início do século XX desencadeou a teorização do poder aéreo e a percepção deste como sendo superior:

> Se o poder marítimo era mais penetrante do que o poder terrestre em razão da grande preponderância dos oceanos em relação aos continentes na superfície terrestre, então o poder aéreo teria de ser mais penetrante do que ambos, pois os aviões podiam, indiferentemente, sobrevoar terra ou mar, e atingir maiores velocidades do que navios e veículos terrestres (WIGHT, 2002, p. 64).

Inicialmente utilizado para missões táticas de reconhecimento, uma vez incorporada nas forças aéreas a execução de bombardeios, o poder aéreo provou ser como uma prática ofensiva eficaz e, capaz de vencer o isolamento, até mesmo, de ilhas remotas (WIGHT, 2002). Na Primeira Guerra Mundial, os aviões tinham limitação de velocidade, carga e segurança, sendo utilizados como força de suporte aos exércitos aliados. No fim dessa guerra, surgiu a visão "da aeronave operando independentemente de exércitos e armadas [...] com o propósito de destruir elementos essenciais da capacidade inimiga de fazer a guerra, pelo bombardeio de fábricas, intercessões de vias de transporte e centros de governo" (MAC ISAAC, 2001, p.217).

Discutir a superioridade de algum dos poderes militares é de pouca importância, como afirmou Wight (2002, p. 66-67), ainda no século XX:

> [...] a crescente unificação do mundo por intermédio de comunicações mais rápidas tornou obsoleto (sic) a velha discussão entre os poderes marítimo, aéreo e terrestre. As três armas têm se tornado cada vez mais interdependentes [...] A administração interna dos [E]stados hoje subordina as três armas a um único Ministério da Defesa; e a estratégia atual enfatiza a necessidade de versatilidade e flexibilidade das armas, para que a força possa ser usada de muitas maneiras diferentes.

Sendo assim, o importante é valorizar todas as forças e entender como cada uma pode ser aproveitada de acordo com o contexto de utilização e os interesses dos Estados. Em certos casos, novas aplicações para as forças existentes ou mesmo novas forças podem surgir, como será explorado na sequência a partir da discussão da ampliação do poder.

2.4 O PODER AMPLIADO PELAS NOVAS URGÊNCIAS DE SEGURANÇA

2.4.1 A segurança no ambiente anárquico

Como produto da anarquia, de acordo com a visão realista, os Estados devem estar preocupados com sua segurança e a possibilidade de serem atacados, dominados ou aniquilados (HERZ, 1950). Isso porque, "*the state of nature is a state of war. [...] with each state deciding for itself whether or not to use force, war may at any time break out*" (WALTZ, 1983, p. 102, grifo nosso). Por causa desta percepção realista das relações internacionais,

“todos os Estados têm de estar constantemente prontos para opor a força à força ou para pagar o preço da fraqueza” (WALTZ, 2004, p. 198).

Nesse sistema anárquico, a guerra é algo potencial de ocorrer. Defendem os realistas que o que ocasionará a guerra e a violência será a presença de um desequilíbrio na distribuição de poder entre os Estados, de modo que em determinado momento um ator estatal, encontrando-se com seu poder militar aumentado e consequentemente com maior potencial de sucesso em caso de agressão, ocasionará um rompimento da estabilidade do sistema. Logo, a paz e a segurança são produtos da manutenção da balança de poder, “seja através do efetivo uso do poder militar (violência) ou da ameaça de utilizá-lo (dissuasão)” (AMARAL, 2008, p. 65).

Se o que ocasiona a guerra é um desequilíbrio de poder entre os Estados, a segurança será medida pela existência de um equilíbrio de poder, especificamente de poder militar. Assim sendo, é possível perceber a visão tradicional da segurança, defendida pela escola realista, em que: a segurança do Estado — principal ator nas relações internacionais — é “medida em termos de seu poder material disponível para lidar com ameaças de cunho essencialmente militar” (WALT, 1991 *apud* AMARAL, 2008, p. 65). É possível depreender dessa acepção de segurança que: i) o objetivo é a sobrevivência do Estado; ii) o poder militar assume preponderância no estabelecimento da segurança; e iii) os outros tipos de poderes nacionais — diplomático e econômico — assumem importância secundária, sendo, portanto, derivados do poder militar (AMARAL, 2008).

Isto posto, torna-se claro o fato de que por causa da condição de anarquia internacional, os investimentos nacionais em instrumentos militares de defesa assumem condição primordial, tendo-se em vista o desejo de garantir que o Estado não seja submetido a adversários e que possa ganhar prestígio ou aumentar seu território.

2.4.2 Novo domínio, nova ameaça

Ao longo da história, avanços tecnológicos marcaram o surgimento de novos exercícios de poder nacional. O domínio do mar ocorreu conforme produziram-se meios que facilitam a navegação dos oceanos, da bússola aos submarinos, passando pelos veleiros e navios a vapor. Aos poucos a teoria do poder marítimo tornou-se mais bem delineada. De

modo semelhante, o domínio da terra e a construção teórica do poder terrestre deu-se à medida que se desenvolveram tecnologias específicas para que o ser humano pudesse explorar militarmente esse meio, até chegar atualmente aos tanques de guerra (KUEHL, 2009).

Com o domínio do ar e do espaço, de forma idêntica, o progresso das formas de transporte e da tecnologia permitiram o estabelecimento humano nesses meios. A Internet foi o grande avanço tecnológico do final do século XX que trouxe profundas modificações nas formas como o mundo conecta-se, relativizando de modo ainda mais intenso as distâncias. Um novo domínio emergiu com esse progresso tecnológico, e além dos quatro domínios físicos — água, terra, ar e espaço — passou-se a considerar um quinto, o espaço cibernético (KUEHL, 2009).

Desse novo domínio, existe uma forte dependência na sociedade atual, a todo momento trocando informações por meio desse espaço. Setores de elevada importância para um Estado e sua sociedade, como transporte, energia e defesa, estão em algum nível sendo controlados por redes de computadores, expostos a vulnerabilidades de exploração de informações e interrupção de serviços. A Internet trouxe diversas vantagens para o cotidiano, apesar disso ela acarretou o surgimento de novas ameaças representadas principalmente pelas atividades infecciosas de vírus e outros códigos de variadas funções facilmente disseminados com capacidade de gerar alto impacto, o que colocou em evidência a necessidade de militarizar o espaço cibernético (HJALMARSSON, 2013). Nesse sentido Kramer (2009) afirma que:

> *The cyberworld is not secure. Each level of cyber—physical infrastructure, operational software, information, and people—is susceptible to security breakdown [...] Periodically, significant virus or denial-of-service attacks are featured [...] the annual number of attacks is extremely large, and they often occur against significant targets* (KRAMER, 2009, p. 6, grifo nosso).

Embora existam muitos atores dependentes dos sistemas informacionais e consequentemente vulneráveis, o enfoque deste trabalho está em analisar a segurança dos Estados, à medida em que o espaço cibernético apresenta-se como meio para concretizar-se invasões em redes de instituições públicas, obter informações, danificar sistemas e potencializar ações militares tradicionais.

O uso do espaço cibernético para o exercício da força e da guerra é resultado da emergência do poder cibernético, cujo desenvolvimento passa a ser exigido por parte dos Estados, de acordo com a lógica realista, para assegurar a sobrevivência e ampliar as possibilidades do Estado de atingir seus objetivos.

2.4.3 O poder cibernético e a garantia da segurança

Buscando a segurança, os Estados são impelidos a adquirir mais poder:

> *This, in turn, renders the others more insecure and compels them to prepare for the worst. Since none can ever feel entirely secure in such a world of competing units, power competition ensues, and the vicious circle of security and power accumulation is on* (HERZ, 1950, p. 157, grifo nosso).

Dentro do realismo o poder é essencial. Para Morgenthau, a meta dos Estados é a "maximização do poder (pois apenas o poder limita o poder), em Waltz a meta última das unidades no sistema internacional é maximização de sua própria segurança, independente[mente] se esta será alcançada reforçando-se o equilíbrio de poder ou abalando-o" (AMARAL, 2008, p. 63-64).

Tradicionalmente, o poder militar entendido, como capacidade de controlar resultados nos domínios terrestre, naval e aéreo, destaca-se na realização das atividades de um Estado que visa a sua sobrevivência no sistema internacional. No entanto, quanto mais poder o Estado tiver, mais condições terá de garantir não só sua sobrevivência, como também de atingir seus interesses. Utilizando-se do poder econômico ou diplomático, a sua política estará pautada na luta por demonstrar quem tem mais condições de influenciar o outro por meio dos instrumentos diplomáticos e econômicos — política do poder. Quando se utiliza do poder militar para garantir sua sobrevivência ou atingir seus interesses, o Estado está colocando em prática a política da força e preservando sua segurança.

Como as relações internacionais são um espaço de luta por poder, o Estado que possuir mais poder, isto é, constituir-se como uma potência, será aquele com maior capacidade de sobrevivência e detentor de mais meios para atingir os resultados almejados ao conseguir controlar demais atores internacionais.

O desenvolvimento, nos últimos anos, de um novo domínio, gerou um novo tipo de poder. É mais um espaço em que o Estado pode projetar sua presença e usá-lo favoravelmente na garantia de sua sobrevivência e na concretização de seus interesses. É o poder cibernético, mais precisamente o poder exercido no espaço cibernético.

Aplicado ao conceito de segurança nacional na perspectiva realista, esse poder serve não só em atos defensivos — ataque e defesa — necessidade imposta pelo ambiente anárquico, mas também em atos que visam o alcance do interesse nacional. O propósito deste trabalho está relacionado ao emprego do poder cibernético no sentido defensivo, isto é, no exercício do poder cibernético militar com o objetivo último de garantir a sobrevivência do Estado.

Por ora, é suficiente perceber que a segurança do Estado é colocada em risco por uma nova ameaça: a de sofrer ataques cibernéticos, conforme o sistema informacional assume elevada importância na sociedade sendo utilizado para controlar inclusive setores críticos do Estado. Surge nesse contexto, o poder cibernético, que, empregado ao militar, assegura a permanência estatal frente aos novos desafios de segurança postos pela emergência do espaço cibernético.

2.5 CONCLUSÕES PARCIAIS

De acordo com a corrente realista, "o objetivo primeiro, último e único dos Estados é maximizar seu poder (MORGENTHAU, 1948) e/ou [sua] segurança (WALTZ, 1979), com vistas a garantir sua sobrevivência em um sistema internacional anárquico e consequentemente, ameaçador (HERZ, 1950)" (AMARAL, 2008, p. 63).

Na teoria realista é central a percepção dos Estados como unidades soberanas travando relações em um ambiente anárquico marcado pelo medo e a desconfiança cuja máxima é a sobrevivência. Decorrente dessa percepção, é clara a colocação do poder como atributo necessário ao Estado e por conseguinte, de seu interesse, sendo razão comum a toda ação política internacional.

Do mesmo modo como o exercício do poder e o desenvolvimento da força terrestre, marítima e aérea são importantes para um Estado dentro da perspectiva realista, a partir do momento em que a noção de que há um novo domínio em que o Estado possui

vulnerabilidades e, portanto, meios de sofrer ataques, torna-se claro que a segurança e sobrevivência do país no atual contexto tecnológico não é mais possível de ser garantida apenas pelas tradicionais forças militares atuando nas tradicionais tipologias, gerando assim a noção de poder cibernético militar e o seu desenvolvimento dentro das estratégias de defesa nacional.

3 PODER CIBERNÉTICO E DEFESA NACIONAL

A emergência do espaço cibernético aprofunda a anarquia internacional e; aumenta a insegurança dos Estados, principalmente por ser um meio que se desenvolve à revelia do Estado, sem sujeitar-se às noções de fronteiras e soberania estatal. Um mundo quase à parte onde se desenvolvem as relações internacionais, porém sobre o qual não se aplicam conceitos do mundo material de governo e onde a ordem não pode ser obtida por coerção física (BARLOW, 1996).

Conforme cresce a dependência de diversos campos e setores do espaço virtual, percebe-se mais claramente que a era digital na qual a atual humanidade está inserida pressupõe ameaças à sobrevivência e à segurança dos Estados nos moldes realistas, requerendo deles uma estratégia de defesa que abranja o meio cibernético.

Tal percepção é acentuada ao se considerar que, do ponto de vista do Estado, estruturas essenciais, como as redes de transportes, comunicação, financeiras, de água e eletricidade, são controladas, em alguma medida, virtualmente e dependem do funcionamento adequado deste meio.

Ao mesmo tempo em que se nota a necessidade de criar capacidades de impedimento de ataque às infraestruturas críticas nacionais, os países também enxergam nesse domínio a possibilidade de usá-lo para fins militares ofensivos e retaliatórios para que, desse modo, tenham mais chances de atingir seus objetivos políticos.

Sendo assim, esta seção, preocupada com a realização do poder cibernético para a segurança do Estado tem dois objetivos 1) levantar os aspectos de vulnerabilidade e de vantagem do espaço cibernético; 2) compreender o poder cibernético e sua correlação com o poder militar.

Para tanto, a discussão a seguir abordará inicialmente os aspectos do espaço cibernético e as ameaças a ele associadas, para então tratar da defesa cibernética a qual se realiza por meio do poder cibernético.

3.1 ESPAÇO CIBERNÉTICO

O objetivo aqui não é trazer uma perspectiva técnica, aplicada aos estudos de Ciência da Computação, mas, sim, abordar uma definição clara para que sejam realizadas as discussões posteriores.

Primeiramente, explorando o termo *cibernética* percebe-se que ele tem sido relacionado ao controle e à comunicação por meio das infovias — sistemas de informação conectados como computadores e celulares — (FERREIRA NETO, 2013). Desse modo, o espaço cibernético é compreendido com base no conjunto de dispositivos eletrônicos conectados em redes, o que não significa que esse ambiente seja sinônimo de Internet ou de Web (FRAZÃO, 2016).

Tanto a Internet quanto a Web são tecnologias que fazem parte do espaço cibernético, contudo este termo é mais abrangente. Desde 1990, diferentes autores têm contribuído para ajudar no entendimento do espaço cibernético compreende. Após realizar um levantamento de diversas das definições propostas por diferentes estudiosos e instituições, Kuehl (2009) definiu o espaço cibernético como:

> " *[...] a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies* (KUEHL, 2009, p. 4, grifo nosso).

Dessa definição, percebe-se como o espaço cibernético diferencia-se de outros aparatos tecnológicos criados anteriormente para facilitar as comunicações. A imprensa, o telégrafo, o telefone, o rádio e a TV trouxeram diversas mudanças para as relações sociais, políticas e militares, ao otimizar o modo como as informações são trocadas. No entanto, foi essa tecnologia mais recente, o espaço cibernético, que foi além do objetivo de transmissão de mensagens, ao permitir que, mais do que simplesmente intercambiadas, as informações possam ser criadas, armazenadas, modificadas e exploradas em um espaço próprio (SHELDON, 2011).

Esse espaço, que é constituído por redes interconectadas e interdependentes, é também bastante complexo, coexistindo tanto nas esferas físicas quanto virtuais, isto é, tanto no espaço geográfico delimitado pelas fronteiras, quanto fora dele, podendo ser distinguidas três camadas distintas, embora correlatas, que formam o espaço cibernético, quais sejam: física, lógica e social.

Primeiramente, a camada física corresponde a sistemas e infraestruturas que permitem a conectividade global — cabos, computadores, roteadores, servidores, entre outros —. Estando dentro de unidades soberanas, o uso dos aparatos dessa dimensão é estabelecido pelas leis de cada país. Tendo em vista que os elementos constitutivos dessa dimensão são produtos das inovações e produções tecnológicas humanas, revela-se uma das características únicas do espaço cibernético que, inclusive, o diferencia dos demais e que corresponde propriamente à vinculação de sua existência com objetos produzidos pelo homem, sem os quais esse meio não seria concebível, em contraste com os outros domínios, cuja existência é dissociada do desenvolvimento de instrumentos para explorá-los e constituí-los (ESTADOS UNIDOS DA AMÉRICA, 2010; CROWTHER, 2018; LIBICKI, 2007; SHELDON, 2011).

Em segundo lugar, a camada lógica é formada por componentes que podem ser transferidos digitalmente e eletronicamente, o que corresponde a Internet e software que promovem a manifestação do mundo virtual, como as páginas Web. Assim, observa-se outra característica singular do espaço cibernético que é a sua dependência do espectro eletromagnético o qual lhe propicia a conectividade e operacionalidade. Nessa camada, o entendimento do exercício da soberania é controverso, com alguns Estados a exemplo da China e da Rússia afirmando possuir soberania também sobre esse novo domínio (ESTADOS UNIDOS DA AMÉRICA, 2010; CROWTHER, 2018; LIBICKI, 2007).

Por fim, a terceira camada, a social, inclui os componentes da *persona* e da *cyber persona,* o que correspondem respectivamente ao indivíduo e à sua identificação no espaço virtual — e-mail, endereço IP, número de telefone, dentre outros —, que estão sujeitos às leis e políticas estatais, assim como os componentes físicos (ESTADOS UNIDOS DA AMÉRICA, 2010; CROWTHER, 2018; LIBICKI, 2007).

A aproximação entre esse espaço cibernético e o poder militar é em função tanto das vantagens tecnológicas associadas a ele em relação aos outros domínios, quanto dos riscos que envolvem esse ambiente (GOMEZ, 2016). Essas vantagens e riscos são perceptíveis nas

características desse espaço e na ocorrência de alguns eventos internacionais, os quais são explorados nas subseções seguintes.

3.1.1 Características particulares do espaço cibernético

Quando comparado aos domínios tradicionais — terra, mar, ar, espaço —, o cibernético possui características únicas que o diferenciam, e por isso, colocam novos desafios para os Estados. Como levantados anteriormente, dois aspectos particulares do espaço cibernético são suas origem humana e dependência eletromagnética. No entanto, existem alguns outros aspectos singulares a esse domínio, abordados a seguir.

Em primeiro lugar, o espaço cibernético é amplamente mais suscetível à mudança do que os outros domínios. Embora avanços tecnológicos promovam aumento das vantagens do poder desenvolvido na terra, no mar, no ar e no espaço, os constantes desenvolvimentos tecnológicos são capazes de acarretar alterações nas forças fundamentais do espaço cibernético, bem como nas condições do próprio meio, o que não acontece com os demais domínios (NYE, 2010; RATTRAY; HEALY 2010).

Em segundo lugar, diferentemente dos ataques realizados contra países, grupos e indivíduos em outros domínios, no espaço cibernético as ações podem assumir um efeito instantâneo, global e além disso anônimo. Essa instantaneidade deve-se à rapidez com que as informações cruzam o espaço cibernético, o qual, estendido pelo mundo, oferece um caráter global. O anonimato tem correlação com a terceira camada do espaço cibernético, já explicada na subseção anterior. Uma vez que existe a *cyber persona*, a identificação no meio virtual não necessariamente corresponde às características reais do indivíduo, e, assim, o espaço cibernético funciona aos moldes de um santuário, oferecendo proteção e encobrindo agressores. Se, nos domínios tradicionais, as ações militares são revestidas por vários fatores de incerteza e de difícil previsibilidade que constituem a névoa da guerra, nos dizeres clausewitzianos, no espaço cibernético a falta de conhecimento sobre o inimigo e suas potencialidades faz-se presente de modo ainda mais intenso, pois frequentemente um Estado pode sofrer ataques sem ter clareza de quem os perpetrou. (CROWTHER, 2018; NYE, 2010; SEWALL, 2007)

Em terceiro lugar, as ações podem ainda acontecer no domínio cibernético sem que haja aplicação de força física, mobilização de diversos equipamentos e suprimentos ou invasão de um território soberano, também sem que precisem ser consideradas condições climáticas e características do território antes de realizarem-se ações nesse espaço (CROWTHER, 2018).

Desse modo, é mais simples concretizar operações no ambiente cibernético, posto que os custos são significativamente menores que aqueles mobilizados para explorar outros domínios e oferecer as condições operacionais necessárias para as tropas das Forças Armadas. Sem a necessidade de orçamentos bilionários e com a facilidade para entrar e sair do espaço cibernético, mesmo Estados pequenos e atores não estatais conseguem atuar nesse domínio e beneficiam-se de vulnerabilidades econômicas e militares, inclusive de grandes atores internacionais. Até mesmo o conhecimento restrito sobre programação não obrigatoriamente atua como impedimento para ação e geração de impacto no espaço cibernético, abrindo margem para que um número ainda maior de atores seja capaz de estabelecer efeitos estratégicos no meio virtual (NYE, 2010; SHELDON, 2011).

Em quarto lugar, o espaço cibernético favorece, em maior grau, as ações ofensivas em relação às defensivas. Isso se explica com base em alguns fatores, tais quais: i) rapidez dos ataques, que, sentidos quase instantaneamente, dão pouco tempo para organização e resposta da defesa; ii) emergência de ofensivas de variadas localidades e de modo anônimo, dificultando a implementação de um contra-ataque; iii) em razão do caráter global do domínio tornando-o amplo o bastante e consequentemente limitando a eficiência da defesa, visto que diversas áreas na sociedade para além do campo militar são dependentes do espaço cibernético (SHELDON, 2011).

Todas essas características do espaço cibernético podem ser entendidas ao mesmo tempo como vantajosas ou potencializadoras de ameaças. Pelo exposto, observa-se, de um lado, que esse domínio se concretiza como fator de insegurança para o Estado, uma vez que é acentuadamente difícil estabelecer um sistema eficiente de defesa, tendo em consideração, especialmente, o anonimato, a instantaneidade das ações e a facilidade de entrada e saída. Por outro lado, as mesmas características que expõem as vulnerabilidades do Estado, dotam-no de diversas facilidades para a realização de ofensivas criando liberdade de ação, motivo pelo qual, nas operações militares atuais, este domínio encontra-se integrado aos quatro outros, de

modo interdependente, com o objetivo de alavancar as capacidades de um Estado e criar efeitos únicos e decisivos (CARNEIRO, 2012).

3.1.2 O espaço cibernético na visão realista

Como este trabalho parte da perspectiva teórica realista, faz-se essencial considerar aqui os aspectos levantados por essa escola ao se abordar o espaço cibernético. Para os realistas, duas concepções importantes que ressaltam nesse domínio são as questões de anarquia e de Estado. O forte caráter anárquico e a falta de fronteiras nos moldes de um território físico são aspectos do espaço cibernético que reforçam suas desconfianças e incredulidades, enxergando nesse meio desafios e vantagens, mas sobretudo fortes ameaças.

A discussão e o entendimento do espaço cibernético pela lente realista tem ocorrido principalmente nos estudos militares e estratégicos, em que se reconhece esse meio como um novo território e como um domínio operacional, em que a falta de governo e o próprio caráter estrutural do espaço acentuam a necessidade de envolvimento dos governos nacionais e das Forças militares para o gerenciamento e controle do território virtual com o objetivo de defendê-lo de possíveis invasões. As desconfianças e incredulidades nas instituições e regimes internacionais realistas são acentuadas nas considerações desse meio em que a anarquia é um aspecto pouco contestável. Duvidando da possibilidade de um regime capaz de regulamentar esse espaço, eles observam que, porquanto diversos interesses estratégicos estejam associados a esse domínio, o Estado encontra-se ameaçado e sua segurança exige proteção e vigilância (MANJIKIAN, 2010).

Para além da insegurança vinda do aspecto anárquico desse novo domínio, os realistas observam as ameaças geradas no nível do indivíduo no espaço cibernético, as quais são resultantes da capacidade desse domínio em mobilizar vastas populações. Eles atentam para o fato de que indivíduos mal intencionados com comportamentos insurgentes, podem ser mobilizados, inclusive estimulados, pelas facilidades do próprio meio, a criar comunidades virtuais globais conectando pessoas com baixa ou mesmo sem identidade estatal, as quais beneficiando-se das características do espaço cibernético de anonimato e de pouca clareza na diferença entre combatentes e não combatentes, passam a articular conflitos irregulares

criminosos, terroristas e de ativismo militar social (ARQUILLA; RONFELDT, 1996; MANJIKIAN, 2010; SAGEMAN, 2008).

Os realistas destacam para além do caráter amorfo — sem fronteiras e anárquico — e do anonimato, a velocidade e o baixo custo de realizar ações nesse espaço mostrando que a capacidade de causar dano atualmente não necessariamente é proporcional ao montante de investimentos, treinamentos, motivação ou desenvolvimento tecnológico (MOSELEY, 2007 *apud* MANJIKIAN, 2010).

Essa desproporção entre investimentos e capacidade de ataque, que os realistas apontam como desvantagem do espaço cibernético, também é abordada como vantajosa, no sentido de que ela promove a multiplicação de força, o que confere a Estados menores capacidades para derrotar um oponente maior. Aprofundando esse aspecto, os realistas mostram que esse espaço permite, também, a redução da densidade de força e do atrito nos campos de batalhas, sobretudo conveniente para países com baixa demografia, baixo contingente militar e vasta área geográfica. No rol das vantagens, eles lembram ainda que o espaço pode ser utilizado como meio de impedir a continuidade do ataque inimigo e de vencer uma guerra não destruindo o inimigo, mas tornando-o incapaz ou pouco disposto a lutar (MANJIKIAN, 2010).

3.1.3 Atores do espaço cibernético

Ainda na discussão sobre as características particulares ao espaço cibernético, torna-se imprescindível tratar também da questão dos atores desse espaço. Como tratado anteriormente, um dos aspectos facilitadores desse meio é a entrada e saída do meio, isto é, as poucas barreiras ao ingresso de novos atores. Estes podem aproveitar-se do caráter relativista de poder nesse meio e, mesmo diante de relações assimétricas, por exemplo contra instituições fortemente amparadas tecnologicamente, conseguirem realizar invasões por meio de software malicioso (malware) recém criado, que os sistemas das vítimas ainda não reconhecem como perigosos e portanto não dispõem de meios de defesa (NYE, 2010).

Esses fatores propiciam que, no meio cibernético, desde jovens com conhecimento em programação, até governos, passando por organizações, grupos criminosos, terroristas e outros invasores ideologicamente motivados, tornem-se atores capazes de ameaçar os

interesses nacionais (KUEHL, 2009). Importante destacar, no entanto, que, embora se constituam como ameaças, atores não estatais oferecem danos comparativamente inferiores aos que governos conseguem colocar em prática (DODGE, INSERRA, 2015).

Grupos criminosos, terroristas e outros invasores podem mobilizar recursos, entretanto, os ataques que eles possam causar não são de elevada preocupação para os Estados, porque não implicam perdas grandiosas aos governos. Os países são as unidades que conseguem reunir maior quantidade de meios, e utilizar-se de agências especializadas de Inteligência e cibernéticas que aumentam as potencialidades de penetração em redes, mesmo se elas estiverem protegidas por códigos encriptados de alta complexidade e, desse modo, infrinjam danos de elevado impacto nas infraestruturas críticas de um país (NYE, 2010; LACHOW, 2009):

> *[...] states benefit from a number of factors and still maintain a distinct advantage in cyberspace. If a small group can acquire a laptop cheaply, then a nation state can acquire an enormous number of laptops, run training programs, and form institutions that reap economies of scale. Nation states can develop relationships with industry. Nation states retain a political legitimacy associated with their use of violence and force within a territory or in line with international rules of war that substate groups lack or must actively campaign for* (BARNARD-WILLS; ASHENDEN, 2012, p. 114-115, grifo nosso).

Desse modo, evidencia-se que no espaço cibernético, a assimetria e a relativização de poder dotam atores não estatais de maior força para operar. Todavia, os Estados, por terem maior acervo tecnológico e contarem com maiores recursos, reúnem consequentemente maior poder cibernético, o que os caracteriza como os principais atores do espaço cibernético e as maiores ameaças quando se considera a possibilidade de um Estado sofrer ataque cibernético.

3.2 ATAQUES CIBERNÉTICOS

As características do espaço cibernético tratadas anteriormente acentuam a insegurança dos Estados, porque propiciam a ocorrência de diversos tipos de ataques. A maior parte dos eventos envolvendo o espaço cibernético são referentes a espionagens e crimes cibernéticos, ataques de baixo custo e pequena complexidade tecnológica, podendo ser desenvolvidos inclusive por atores sem motivações fortes (CSIS; UNIDIR, 2016; NYE, 2010).

Os ataques de maior risco implementados até hoje totalizam número bem inferior. Eles possuem propósitos diferentes da espionagem e dos crimes e buscam frequentemente interromper sistemas complexos e causar destruição física. Normalmente, são os sistemas operacionais militares e as infraestruturas críticas que podem ver-se afetadas em alta gravidade nesses ataques, os quais envolvem atores estatais (CSIS; UNIDIR, 2016; NYE, 2010). Entre os eventos de maior risco já acontecidos, destacam-se os casos da Estônia em 2007, da Geórgia em 2008 e do Stuxnet em 2010 (BERWANGER, 2015).

O ataque da Estônia em 2007 é considerado como o "primeiro ato de ciberguerra" (BERWANGER, 2015; NYE, 2010) e precursor dos impactos que um ataque cibernético pode gerar sem que, para isso, forças convencionais sejam mobilizadas. Ocorreu no contexto de um conflito étnico em que a minoria russa se opôs à decisão da maioria estoniana de retirar uma estátua de bronze de um soldado do Exército Vermelho feita em homenagem aos militares soviéticos mortos nos combates contra o nazismo. A estátua era um símbolo do passado comunista do país, dos anos que ele fez parte da União Soviética e da ocupação russa. Após a retirada da estátua, *sites* do governo, de bancos e de jornais saíram do ar, logo depois de receber milhares de visitas por segundo, sob um ataque de negação de serviço distribuído (DDoS). O *site* do governo estoniano, por exemplo, que normalmente recebia entre 1000 e 1500 visitas por dia, chegou a receber o mesmo número de acessos por segundo (CLARKE; KNAKE, 2010; RITUERTO, 2007). A Estônia imputou a Rússia como a autora mais provável dos ataques, porém pelas dificuldades próprias do meio cibernético, não conseguiu provar tal alegação.

Outro ataque cibernético notório foi o realizado pela Rússia contra a Geórgia em 2008. Na ocasião, os geórgicos haviam invadido a Ossétia do Sul, por não aceitar sua independência recém declarada. Os russos, apoiando a Ossétia do Sul, lançaram ataques DDoS contra *sites* do governo e midiáticos da Geórgia, além de instituições financeiras, empresas, de ensino e da mídia ocidental, como BBC e CNN. Em alguns ataques, não só incluíram negação de serviço, como também modificação dos *sites (defacement)*, a exemplo de publicações pró-Rússia nas páginas do governo. Enquanto os ataques eram implementados, o exército russo avançava e promovia, inclusive, bombardeios sobre a Geórgia, sendo "o primeiro caso em que um conflito internacional político e militar, foi acompanhado, ou mesmo precedido por uma ofensiva de ataques cibernéticos" (GRAÇA, 2013, p.34). Similarmente ao caso da Estônia, a

Rússia foi considerada pela Geórgia como a responsável mais provável pelos ataques, contudo também não foi possível provar.

O caso do Irã por seu turno, foi, dos três casos explorados aqui, o mais complexo, pois envolveu o desenvolvimento de um *malware* capaz de invadir e controlar sistemas industriais de infraestruturas críticas. A qualidade do espaço cibernético como meio útil para oferecer suporte à consecução de atos violentos ao longo de conflitos estatais já fora reconhecida e aproveitada. No entanto, o Stuxnet ensejou o primeiro momento em que se constatou o meio virtual como alternativa para aplicar danos físicos a adversários. (GOMEZ, 2016)

O Stuxnet é um malware, descoberto em 2010, que foi introduzido no sistema nuclear do Irã, onde controlou a velocidade de rotação das centrífugas de enriquecimento de urânio por quase um ano, para causar danos ao maquinário e atrasar o programa nuclear que o país vinha desenvolvendo (BERWANGER, 2015; DODGE, INSERRA, 2015). Esse vírus é considerado uma arma cibernética de caráter militar, desenvolvida para destruir as centrífugas de refinação nucleares iranianas, tendo conseguido inutilizar cerca de 1000 delas (CLAYTON, 2011). Acredita-se que os EUA e Israel foram os responsáveis pelo caso, tendo envolvido alto investimento por cerca de seis meses em uma equipe entre 8 e 10 pessoas. A autoria, no entanto, nunca foi confirmada (SCHNEIER, 2010).

3.3 SEGURANÇA E DEFESA CIBERNÉTICAS

Percebe-se que algumas características do espaço cibernético são desvantajosas para os Estados por ameaçarem a continuidade da sua segurança e a possibilidade de alcançar seus interesses. O baixo custo para empreender ataques cibernéticos e o anonimato do meio virtual facilitam a ocorrência de ofensivas nesse meio, envolvendo terrorismo, crime, espionagem, ataques e, nos casos mais graves, destruição de sistemas e unidades físicas.

Esses riscos somados à ocorrência de ataques concretos como os da Estônia, da Geórgia e do Irã contribuem para que, na contemporaneidade, os Estados entendam a importância de desenvolver capacidades cibernéticas, associá-las ao poder militar e, deste modo, defender o espaço cibernético (BERWANGER, 2015). O caso do Stuxnet no Irã, principalmente, foi notório no sentido de afirmar o caráter ofensivo do espaço cibernético e sua relação com as esferas políticas e militares estatais (GOMEZ, 2016). Ficou mais clara,

para a comunidade internacional, a possibilidade de que não só haja conflitos no espaço cibernético, mas de que também possam ocorrer guerras cibernéticas (BARNARD-WILLS; ASHENDEN, 2012).

A elevada intenção maléfica junto ao aumento da suspeita de que grande número de países estava empenhado em realizar operações ofensivas cibernéticas incitara de modo mais enfático, a percepção que vinha sendo construída sobre a indispensabilidade de atribuir a segurança do espaço cibernético a organizações estatais especializadas voltadas à defesa militar (GOMEZ, 2016).

Nesse sentido, introduziram-se, mundo afora, noções e políticas de segurança e defesa cibernéticas. Segurança Cibernética diz respeito "ao combate e à prevenção dos chamados crimes cibernéticos na esfera da segurança pública" (SOUZA, 2013), isto é, ações das quais cidadãos e entidades públicas ou privadas são as vítimas, seja roubo de dados, seja acesso a contas bancárias ou a dispositivos móveis de uso pessoal, dentre outros casos. Já Defesa Cibernética, por sua vez, está relacionada "ao conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético", (CARVALHO, 2011, p. 8 a*pud* SOUZA, 2013, p. 27), sendo, portanto, atrelada às Forças Armadas. Trata-se da proteção dos sistemas militares e das infraestruturas críticas — energia, telecomunicações, transportes —, redes cuja desativação seria capaz de causar danos incalculáveis aos países.

O presente estudo, partindo da teoria realista, volta-se para o ator estatal e a realização de seu poder para garantir sua segurança e objetivos políticos. Logo, interessa aqui não a Segurança Cibernética, mas, sim, a Defesa Cibernética, uma vez que esta envolve diretamente o Estado e o poder militar.

A Defesa Cibernética, para ser concretizada, requer que o Estado possua capacidade de atuação no espaço cibernético, isto é, desenvolva poder cibernético. A seguir, será discutido o poder cibernético e sua colocação de modo estratégico no espectro do poder militar, de modo a garantir a proteção das infraestruturas críticas e sistemas militares, além de favorecer os Estados na realização de seus objetivos.

3.4 PODER CIBERNÉTICO

Explorado o conceito de espaço cibernético, avalia-se que suas características são perceptíveis as vulnerabilidades, bem como as potencialidades que ele implica. Combater as ameaças desse meio e aproveitar-se de suas vantagens só é possível pelo exercício de poder nesse ambiente. Deter poder cibernético significa, de acordo com o Realismo, e dentro das realidades colocadas pela emergência do espaço cibernético, a possibilidade de garantir que os países consigam acessar as vantagens únicas dessse ambiente e consequentemente aumentarem as chances de atingir seus objetivos e garantir sua segurança, por meio da Defesa Cibernética.

O poder cibernético pode ser entendido como "*the ability in peace, crisis, and war to exert prompt and sustained influence in and from cyberspace*" (SHELDON, 2015, p. 306, grifo nosso) ou como "*the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of powe*r" (KUEHL, 2009, p. 12, grifo nosso). Em outras palavras, é a capacidade de atingir resultados por meio do uso do espaço cibernético, isto é, do uso de instrumentos informacionais eletronicamente interconectados, criando com isso um contexto por ele gerenciável de contínua vantagem.

Como aborda a definição acima, é um poder que tanto pode ser utilizado especificamente dentro do ambiente cibernético como pode ser estendido aos demais ambientes e poderes, o que evidencia sua capacidade de gerar impacto dentro e fora do ciberespaço e de integrar os diferentes instrumentos de poder estatais (KUEHL, 2009; NYE, 2010). Isso se deve ao fato de que o uso do espaço cibernético está difundido na execução de um amplo espectro de atividades sociais, políticas econômicas e militares, o que torna todas as outras formas de poder estatal vulneráveis à interrupção e à perda de capacidades de atuação nesse meio (KUEHL, 2009).

Resgatando a discussão sobre poder nacional, realizada na primeiro seção, percebeu-se que, dentro do Realismo, destacam-se três tipos de poder estatal, quais sejam: o diplomático, o econômico e o militar. Entendendo-se pela definição supracitada de poder cibernético que ele infuencia os demais poderes nacionais, conclui-se, portanto, que tanto o poder diplomático quanto o econômico e o militar veem-se afetados pelo cibernético. A diplomacia tornou-se mais efetiva, com os países e embaixadas podendo realizar comunicações quase instantâneas e conseguindo tratar problemáticas mais rapidamente. Ao mesmo tempo, tem-se o mundo

diplomático afetado em outros quesitos pelo espaço cibernético, a exemplo da Primavera Árabe, fortemente influenciada pelas mídias sociais. Do ponto de vista econômico, surgem, atreladas a esse espaço, multinacionais tecnológicas que se agregam aos recursos e à economia de seus países sede, enquanto as operações do sistema financeiro e o próprio comércio crescem em dependência do funcionamento do espaço virtual (CROWTHER, 2018; FRAZÃO, 2016).

Em relação ao poder militar, foco do presente trabalho, a interferência do poder cibernético é incontestável diante das vantagens e das vulnerabilidades que o espaço cibernético implica. No rol das vantagens, o poder cibernético associa-se ao militar pela introdução de diversos instrumentos que melhoram a capacidade de comando e controle global das forças e operações. Além disso, ele tem sido pensado como uma estratégia inicial em ações militares. Por exemplo, o conflito ocorrido entre Israel e Síria em 2007 em que aquele bombardeou esta após desabilitar, por meio do espaço cibernético, a rede de defesa aérea de Damasco. Durante o bombardeio da Força Aérea israelense, os radares sírios não acusaram o que estava acontecendo, nenhum dos controles demonstrou que havia alvos e que eles estavam sob ataque (CLARKE; KNAKE, 2010).

No rol das vulnerabilidades do meio cibernético, o poder cibernético torna-se imprescindível para garantir que as estruturas nacionais dependentes do funcionamento de sistemas informacionais não sejam prejudicadas em decorrência de ataques cibernéticos. Contemporaneamente, embora não haja unanimidade entre Estados e estudiosos, são fortes as crenças de que, no futuro, será real a ocorrência de guerras cibernéticas (BERWANGER, 2015), pois “há todas as razões para acreditar que a maioria das guerras cinéticas no futuro serão acompanhadas de guerra cibernética, e que outras guerras cibernéticas serão conduzidas de 'maneira pura', sem explosões, infantaria, poder aéreo e marinhas” (CLARKE; KNAKE, 2010, p. 21).

Apesar disso e da importância que o espaço cibernético assume nas relações internacionais atuais, Valente (2007 *apud* FRAZÃO, 2016) defende que o Estado continua com o espectro tradicional de possibilidades para aplicar seu poder nacional militar, econômico e diplomático, que em seu estudo, ele chama de político, porém as características são as mesmas levantadas na seção anterior para o poder diplomático. Na perspectiva desse estudioso, o espaço cibernético, na manutenção do poder estatal, não opera sozinho e é

exatamente por ser dependente de outras estruturas que ele não pode ser entendido como uma quarta esfera de ação do poder.

Aqui cabe lembrar a hipótese deste trabalho: a incorporação do poder cibernético ocorre de modo complementar às estratégias militares convencionais. Na hipótese levantada, sugere-se que o poder cibernético direcionado especificamente à Defesa Cibernética não existe desassociado do militar, isto é, não é proposta a noção de que o poder cibernético como nova categoria de poder nacional, mas, sim, como nova categoria dentro do poder militar. Uma vez no espectro de poderes militares existentes, ele se junta aos poderes aéreo, marinho e do terrestre dotando as Forças convencionais com maior capacidade de ação ofensiva e defensiva.

A hipótese será realmente analisada e colocada à prova em completude na próxima seção com o estudo das estratégias de defesa dos Estados Unidos no governo Obama. Oportunidade em que mostrar-se-á a aproximação entre poder militar e cibernético naquele país e, também, será possível identificar como os seus principais documentos de estratégia de segurança e defesa nacional direcionam o tema de defesa e poder cibernético.

3.5 CONCLUSÃO PARCIAL

O espaço cibernético enseja vantagens e ameaças aos Estados as quais exigem o desenvolvimento de capacidades para atuar neste novo ambiente. Com sua segurança e alcance de interesses ameaçados, dentre outros fatores, pelo baixo custo para empreender ataques cibernéticos, o anonimato do meio virtual e a alta dependência de suas infraestruturas críticas do espaço cibernético os países voltam-se para a realização de sua defesa cibernética.

4 ANÁLISE DO PODER CIBERNÉTICO DURANTE O GOVERNO OBAMA

No primeiro capítulo foi visto que os Estados buscam maximizar seu poder e/ou segurança (AMARAL, 2008; MORGENTHAU, 1948; WALTZ, 1979). Objetivos que no contexto tecnológico atual não são garantidos detendo-se apenas as tradicionais forças militares, o que impele ao desenvolvimento de poder cibernético.

Tendo-se entendido a relação entre o poder cibernético e o estabelecimento da segurança do Estado como visto no capítulo anterior, esta seção abordará por meio do Estudo de caso dos Estados Unidos a incorporação do poder cibernético à estratégia militar de defesa. É um modo de mostrar como que um dos países mais fortes no tema Segurança e Defesa Cibernéticas articulam suas potencialidades militares para defender o domínio cibernético.

De acordo com o *Global Cybersecurity Index (GCI)* de 2017 produzido pela União Internacional de Telecomunicações (UIT), agência das Nações Unidas (ONU) especializada em tecnologias de informação e comunicação os Estados Unidos são considerado o país com a melhor performance para lidar com as questões de segurança cibernética. O país obteve a melhor pontuação no índice produzido em quatro dos cinco pilares parâmetros da pesquisa realizada com base em dados de 134 países. Assim nos aspectos legais (existência de instituições legais e estruturas voltadas para segurança e crimes cibernéticos); técnicos (existência de instituições técnicas e estruturas voltadas para segurança cibernética); organizacionais (existência de instituições de coordenação de políticas e estratégias para o desenvolvimento de segurança cibernética no nível nacional); e de criação de capacidades (existência de pesquisa, programas, profissionais e agências públicas voltadas para a educação e treinamento em segurança cibernética). Sendo assim os EUA são os países mais avançados no tema de segurança cibernética. (UIT, 2017)

Na contemporaneidade, as tecnologias de comunicação e informação são partes essenciais do funcionamento dos países perpassando níveis econômicos, sociais e militares, uma vez que correspondem desde dispositivos como computadores e celulares pessoais até sistemas de supervisão e aquisição de dados (em inglês Supervisory Control and Data Acquisition - SCADA) que controlam o funcionamento de infraestruturas, por exemplo. Nos Estados Unidos, essas tecnologias além de estarem difundidas nas esferas econômicas e sociais também estão enraizadas no poder militar (SHELDON, 2015).

Como o objetivo deste trabalho é entender como ocorre a incorporação estratégica do poder cibernético no militar, os Estados Unidos, os quais estão fazendo essa incorporação a alguns anos, e possuem hoje as estruturas mais avançadas para lidar com os casos de defesa cibernética, foram escolhidos para estudo mais detalhado no presente trabalho, servindo para enriquecer e exemplificar a discussão proposta.

Observar o modo como a estratégia americana absorve e aplica o poder cibernético é importante para entender a forma como conflitos contemporâneos estão tornando-se mais complexos e para vislumbrar aspectos sobre como conflitos futuros serão realizados e como preparar-se para eles.

O capítulo buscará demonstrar primeiramente como ocorreu a aproximação do poder cibernético ao poder militar americano a partir das mudanças de concepções sobre a importância do espaço cibernético e a necessidade de criar meios capazes de defendê-lo bem como realizar ofensivas. Em seguida, serão abordados os principais documentos da estratégicos do país para efetivamente cumprir o objetivo proposto para esse capítulo e assim elucidar como os EUA inserem estrategicamente o poder cibernético em seu poder militar. O objetivo aqui não é fazer um estudo exaustivo dos documentos e discursos oficiais dos EUA sobre a questão da defesa cibernética, mas mostrar como os principais documentos do período Obama trataram as questões cibernéticas.

4.1 APROXIMAÇÃO DO PODER CIBERNÉTICO AO MILITAR

Nesta seção o objetivo é levantar alguns aspectos importantes para explicitar como ocorreu o processo de militarização do espaço cibernético nos EUA. Para tanto, a seguir serão explorados quatro pontos que ajudam a entender esse processo. Primeiramente, será tratada a criação da Internet, produto de uma política do Departamento de Defesa americano. Em segundo lugar, destacar-se-á a ocorrência da Revolução nos Assuntos Militares que reforçou e colocou em evidência o uso de novas tecnologias. Em terceiro lugar, será mostrado o processo que levou ao entendimento do ciberespaço como domínio operacional. Em último lugar, serão exploradas ameaças do meio que passaram a ser sentidas conforme foram crescendo as potencialidades de possíveis adversários de realizarem conflito no ciberespaço e foram tornando-se mais recorrentes e evidentes os ataques cibernéticos.

Antes de propriamente começar o esclarecimento de cada um dos pontos, importante fazer a ressalva de que os quatro aspectos para explicar a incorporação do poder cibernético no militar dentro dos EUA são extremamente interconectados e em alguns momentos quase indivisíveis, ainda assim optou-se por separá-los com a intenção de desenvolver o objetivo da seção de modo claro.

4.1.1 A criação da Internet

O espaço cibernético, desde sua origem, tem uma relação intrínseca com o poder militar. Isso pode ser visto tratando-se da criação da Internet, parte fundamental e condicionante da existência do ciberespaço, embora não seja a única camada constituinte do meio, como discutido no capítulo anterior. O Departamento de Defesa buscava melhorar seu sistema de comando e controle, para tanto financiou uma organização de pesquisa e defesa, a Advanced Research Projects Agency (ARPA). O resultado desse investimento, foi a Internet, inovação tecnológica de 1969. No contexto da Guerra Fria, a criação dessa rede inicialmente chamada "ARPANET" significava avanços importantes na corrida espacial, armamentista e ideológica contra a União Soviética, a qual tinha acabado de lançar o satélite Sputnik. (REINO, 2015)

Fortemente relacionado ao poder militar desde sua criação, o espaço cibernético tanto pode ser visto como vantagem para a esfera militar (motivo pelo qual foi inicialmente pensado e desenvolvido), bem como pode ser visto quanto às vulnerabilidades que implica. Em relação às vantagens, está a ocorrência da Revolução nos Assuntos Militares, o segundo ponto a ser discutido nesta seção.

4.1.2 Revolução dos Assuntos Militares

A inserção do espaço cibernético no poder militar ocorre de modo mais profundo nos Estados Unidos, sobretudo a partir da Revolução nos Assuntos Militares (RAM). Os EUA têm passado por uma revolução militar em que a tecnologia têm assumido um papel cada vez mais primordial. A RAM teve sua origem nos Estados Unidos a partir de dois confrontos que impuseram-se a eles na segunda metade do século XX: a Guerra do Vietnã e a Guerra Fria. Após anos envolvidos em um conflito extremamente sangrento no Vietnã, sofrendo com

sucessivas derrotas, os americanos mesmo tendo mobilizado grandes investimentos viram-se sem outra opção que não fosse a de aceitar o cessar fogo e retirar suas tropas do território vietnamita. O fracasso na guerra contra a Frente Nacional para a Libertação do Vietnã junto ao conflito contra a União Soviética, que naquele momento contava com paridade nuclear e detinha grande capacidade bélica, impeliram os Estados Unidos a buscar meios de criar vantagens aproveitando-se dos avanços tecnológicos e de novas doutrinas de guerra. (SHIMKO, 1985; MCNAB, WIEST, 2016)

Neste contexto, a RAM emergiu no sentido de que fossem melhoradas as capacidades e tecnologias das Forças Armadas de modo a diminuir vulnerabilidades, proteger a integridade física dos combatentes e tornar o processo de reconhecimento até ataque do adversário mais rápido e preciso. Pelo uso de tecnologias cibernéticas, interfaces de vigilância, redes de comunicação, bem como aparatos de controle remoto, a exemplo dos drones, a estratégia da guerra foi repensada. O modo de realizar-se a guerra ganhou a noção de diminuição e até mesmo de eliminação da fricção no combate, uma vez que a concretização das ações operacionais, táticas e estratégicas começaram a ser pensadas de modo que pudessem apoiar-se mais nos dispositivos tecnológicos e no uso simultâneo dos diversos domínios e capacidades. Esperava-se com isso, aumentar as possibilidades de atingir-se os objetivos iniciais dos engajamentos de modo mais rápido mediante enfraquecimento do inimigo. (SHIMKO, 1985; PERON, 2016)

A RAM correspondendo à aproximação das tecnologias com a defesa, isto é, à maior interoperabilidade entre soldados e novas armas tecnológicas trouxe alterações aos métodos operacionais, o que permitiu a inclusão do espaço cibernético nas operações militares e na condução da guerra. (PERON, 2016). A ocorrência da Revolução nos Assuntos Militares nos EUA durante os anos 1980 e 1990 destacou os aspectos vantajosos de utilizar-se do espaço cibernético na esfera militar, incentivando a incorporação do poder cibernético no militar. Ainda em 1982, os Estados Unidos utilizaram-se do ambiente virtual para introduzir um software defeituoso no sistema de controle dos gasodutos soviéticos. O programa modificado aumentou a pressão dentro das tubulações de gás da URSS causando sua explosão. (DODGE, INSERRA, 2015)

4.1.3 O espaço cibernético como domínio operacional nos EUA

Resultado das políticas levantadas pela RAM, a noção de que o espaço cibernético pode ser um ambiente operacional passou a ser pensada nos EUA principalmente a partir da Guerra do Golfo. Em 1990, antes de iniciar a guerra contra o Iraque, já era discutida a possibilidade de tornar indisponível radares de defesa aérea e redes de mísseis iraquianos como preparação do campo de batalha para que em seguida aeronaves americanas e aliados dessem início a suas ofensivas em Bagdá. Todavia, foi após essa guerra, que o espaço cibernético foi gradativamente tornando-se mais associado ao poder militar no sentido de ser utilizado para a realização de uma guerra cibernética, quando a Força Aérea americana instituiu o seu *Info War Center* e em 1995 formou-se a primeira turma de oficiais treinados para guerras cibernéticas na National Defense University (CLARKE; KNAKE, 2010).

Na Guerra do Kosovo ocorrida entre 1998 e 1999, a Força Aérea conduziu ataques cibernéticos contra o sistema de defesa sérvio, contudo mesmo nesse momento, ainda não estava claro o uso do espaço cibernético como um ambiente operacional. Assim, as ações aplicadas contra a Sérvia foram criticadas pela ineficiência, porquanto o uso de tecnologias para penetrar nos sistemas do inimigo era uma capacidade nova para a qual não havia uma estratégia clara associada capaz de tornar a potencialidade de penetração em redes dos adversários em real vantagem. (BENDRATH, 2001)

Foi no segundo mandato de George W. Bush que a importância do espaço cibernético como um espaço de combate tornou-se mais aparente e foi a Força Aérea dos EUA que deu início ao aprofundamento dessa percepção. Ela criou em 2007 uma unidade para guerra cibernética (Air Force Cyber Command) e defendeu que sua missão era controlar o espaço cibernético, tanto para defesa quanto ataque. Em 2009, o Pentágono convencido do valor da guerra cibernética e da necessidade de dominar o espaço cibernético criou o U.S. Cyber Command (USCYBERCOM), composto por todas as Forças e subordinado a um comando já existente o Strategic Command - STRATCOM. Desse modo, as unidades de guerra cibernética individuais de cada uma das Forças (Aérea, Marinha e Exército) continuaram a ser desenvolvidas, mas a partir de então conduzidas de acordo o U.S. Cyber Command, que por sua vez estava abaixo do STRATCOM. A National Security Agency - NSA, criada em 1952, com expertise em penetração de redes e coleta de informações, porém não autorizada a alterar dados ou se engajar em guerra causando interrupção de serviços ou danos em redes, passou a

dar suporte ao comando cibernético dos Estados Unidos deixando para as unidades de combate militar a responsabilidade de engajamento em guerra cibernética (BERNART JUNIOR, 2012; CLARKE; KNAKE, 2010).

4.1.4 A percepção das ameaças do espaço cibernético nos EUA

A apropriação do espaço cibernético pelo poder militar deve-se não só às vantagens que ele pode implicar (rapidez, precisão nos ataques, diminuição da fricção), mas também ao crescente entendimento de que esse meio precisa ser defendido militarmente, exigindo para tanto a criação de capacidades militares específicas (BERWANGER, 2015).

Em caráter inicial o uso da Internet era restrito aos Estados Unidos, com a ARPANET interligando apenas computadores de instituições de pesquisa e de organizações militares. Com o passar dos anos e com o crescimento da Internet, outras agências governamentais e países passaram a aproveitar da nova tecnologia. À medida em que o espaço cibernético foi sendo expandido, cresceu o número de invasões em sistemas voltadas para espionagem, crimes, destruições cibernéticas (malwares) e físicas. Acentuaram-se, assim, as características particulares do meio virtual (rapidez, anonimato, alcance global, facilidade para ações ofensivas) e a percepção de que infraestruturas críticas e sistemas militares estavam em risco (BERNART JUNIOR, 2012; DODGE, INSERRA, 2015).

Esses fatores associados à crescente capacidade cibernética de adversários geopolíticos também foram sendo associadas à ameaças aos interesses americanos. Foi-se tornando mais claro que do mesmo modo que os EUA poderiam utilizar-se do espaço cibernético na tentativa de atacar e coagir adversários, armas cibernéticas poderiam ser utilizadas contra eles por atores como Rússia, China, Israel, Irã ou grupos terroristas como uma demonstração de força, ou com o propósito de destruir e aterrorizar (BERNART JUNIOR, 2012; DODGE, INSERRA, 2015; CLARKE; KNAKE, 2010).

De fato, alguns adversários como a Coreia do Norte, Rússia, Irã e China têm desenvolvido capacidades cibernéticas e testado contra os EUA. Antes do governo Obama, iniciado em 2009, os Estados Unidos já haviam sofrido vários incidentes cibernéticos, a maioria não foi possível determinar autoria, porém em relação a outros ataques havia a suspeita de que a Rússia ou a China fossem as responsáveis. Nesses incidentes deficiências na

defesa cibernética americana foram exploradas, e com isso seus autores foram bem sucedidos na obtenção de dados e negação de serviços (CSIS, 2017).

Ataques cibernéticos ocorridos na primeira década do século XXI reforçaram essa percepção do espaço cibernético como ameaça. Os ataques sofridos pela Estônia em 2006 e pela Geórgia em 2007 influenciaram o estreitamento entre o poder cibernético e militar nos EUA, tanto porque foram atos realizados pela Rússia, país com o qual os americanos possuem um histórico de rivalidades, quanto porque foram ataques que comprovaram a capacidade e a disposição russas de enfraquecer opositores por meio do uso das tecnologias cibernéticas.

Para além desses casos externos aos EUA, contribuíram para a percepção do espaço cibernético como ameaça episódios relevantes de ataques cibernéticos que eles mesmos viveram. Em 2009, a Coréia do Norte que vinha fazendo demonstrações de poder, entre as quais a explosão de uma bomba nuclear pela segunda vez, no dia da comemoração da independência dos Estados Unidos, 4 de julho, lançou sete mísseis de curto alcance e pouco antes lançou um ataque cibernético contra os EUA. Usaram de um vírus botnet para causar um ataque distribuído de negação de serviço. Alguns sites americanos receberam mais de 1 milhão de pedidos de acesso por segundo, o que ocasionou a queda de alguns sites, entre eles do Departamento de Segurança Interna, do Ministério da Fazenda e do Serviço Secreto. Não houve grandes danos e serviços importantes não foram interrompidos. O governo dos EUA não atribuiu os ataques diretamente a Coréia do Norte, apesar das suspeitas, pela dificuldade de precisar a origem das ameaças, no entanto alertaram-se para o fato de que os ataques sofridos podiam ser apenas demonstrativos do país adversário, o qual já vinha demonstrando sua força em outros domínios (CLARKE; KNAKE, 2010).

Em meio a essas circunstâncias, em 2005, a *National Defense Strategy* identificou o espaço cibernético como um novo teatro de operações que demandava controle para lidar com "*traditional, irregular, catastrophic or disruptive threats*" (RATTRAY, EVANS & HEALY, 2010, p. 139 *apud* BARNARD-WILLS; ASHENDEN, 2012, p. 113, grifo nosso)

4.2 A AMPLIAÇÃO DO PODER MILITAR: PODER CIBERNÉTICO INCORPORADO ESTRATEGICAMENTE

Retomando aqui brevemente a discussão do primeiro capítulo, percebeu-se a importância do poder, isto é, da capacidade de um Estado afetar outros impulsionando-os a fazer o que normalmente não fariam. Foi tratada o poder militar, ou seja, o uso da força para os objetivos políticos No ambiente anárquico em que o espaço cibernético apresenta-se como ameaça recente, naturalmente os Estados são levados a ampliar seu poder militar (suas capacidades de empregar a força para influenciar outros Estados e aumentar sua defesa) a partir da incorporação do poder cibernético.

Sendo o país mais avançado em tecnologia militar, os Estados Unidos usam o espaço cibernético em diversas áreas críticas em que as Forças Armadas operam, incluindo: sistemas de controle, comando, comunicações e inteligência; operações terrestres, aeronáuticas, navais e ofensivas cibernéticas; sustento de operações militares e pesquisa. Para além das estruturas militares, outros setores de infraestruturas críticas do país são dependentes do espaço cibernético como químico; comercial; comunicações; barragens; indústria de defesa; serviços emergenciais; energia; serviços financeiros; sistema de saúde; reatores, materiais e resíduos nucleares; sistemas de transportes, de abastecimento de água, entre outros (DODGE; INSERRA, 2015).

As ameaças mais agressivas dentro desse domínio, normalmente, estão associadas a outros Estados, por serem atores com mais recursos que muitas organizações criminais, corroborando com o explicitado no segundo capítulo. No espaço cibernético desenrolam-se crimes e espionagens que custam bilhões de dólares para os EUA. No entanto, o maior risco não está relacionado a esses ataques, mas aos que podem provocar efeitos equivalentes ao uso da força, cujos alvos mais prováveis são as infraestruturas críticas, especialmente de energia, de telecomunicações, financeira, serviços do governo e de transportes (CSIS, 2017).

No anexo 1 está disponível uma tabela produzida pela Heritage Foundation que reúne os países que constituem as maiores ameaças à defesa cibernética americana, colocando ataques que ele já realizaram tanto aos sistemas dos EUA quanto a outros países. Na tabela ainda é possível identificar os efeitos dos principais ataques, quanto ao entendimento do nível em que geraram impacto, se político, econômico ou militar (Ver Anexo 1).

O subtópico a seguir analisa os principais documentos estratégicos do período Obama (2009-2016) para entender como os EUA vêm se organizando nacionalmente e militarmente para lidar com as ameaças cibernéticas.

4.2.1 Medidas de Segurança e Defesa cibernéticas do governo Obama (2009-2016)

Antes do início da administração de Obama em 2009, os EUA já haviam adotado algumas iniciativas e políticas relacionadas à segurança cibernética, como a *National Strategy to Secure Cyberspace* de 2002, a *National Infrastructure Protection Plan* de 2006, a *National Strategy for Information Sharing* de 2007 e a *Comprehensive National Cybersecurity Initiative* em 2008. Apesar desses esforços, um relatório do CSIS produzido no final de 2008 para o presidente Obama que assumiria no ano seguinte afirmou que a segurança cibernética estava figurando como um dos elementos menos desenvolvidos pela política americana, o que deveria ser superado para que desse modo o país pudesse obter benefícios na promoção de seus objetivos e ainda reduzir os riscos associados à sua segurança (GAD; AUSTIN, 2010).

Em 2009, os Estados Unidos inseriram a segurança cibernética na política nacional de segurança, posicionando as infraestruturas digitais como uma prioridade na segurança estratégica nacional em face dos desafios que o meio cibernético impõem para a economia e a segurança do país (BARNARD-WILLS; ASHENDEN, 2012; NATIONAL SECURITY COUNCIL, 2010) .

Produto desse novo contexto foi a determinação de responsabilidades de segurança e defesa cibernética para algumas instituições nacionais, sendo as duas mais relevantes sobre o tema o *Department of Homeland Security (DHS*) e no *Department of Defence (DoD)*. É de responsabilidade do DHS proteger, prevenir e recuperar o domínio cibernético em caso de incidentes; proteger as infraestruturas críticas e sistemas civis federais; enquanto cabe ao DoD a defesa de suas redes, sistemas e informações; defesa da nação contra ataques cibernéticos; apoio à operações militares e missões ofensivas no espaço cibernético quando direcionadas pelo presidente (UNIDIR, 2013).

As Forças militares além da estratégia conjunta possuem cada uma sua doutrina e estratégia para tratar das questões cibernéticas que afetam suas estruturas diretamente. Dentro

do DoD, os serviços cibernéticos de cada força (U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, 24th Air Force, U.S. Coast Guard Cyber Command e U.S. Marine Corps Forces Cyber Command) constituem o U.S Cyber Command (USCYBERCOM) que como citado anteriormente desde 2009 existia como um sub-comando do U.S Strategic Command (STRATCOM), porém desde maio de 2018 foi dissociado e assim consegue coordenar seus esforços com outros comandos sem passar pelo STRATCOM. Entre outras funções o CYBERCOM pode realizar todas as operações militares de defesa e ofensa no espaço cibernético, inclusive as que envolvam outros domínios; promover treinamentos, realizar pesquisa e desenvolvimento de capacidades (CROWTHER, 2018).

Também resultado do novo contexto foram alguns documentos importantes contemplando ou totalmente voltados para a estratégia cibernética, entre os quais destacam-se: em 2009, a *Cyberspace Policy Review*, contemplada em vários aspectos na *National Security Strategy* de 2010 (UNIDIR, 2013); em 2011: *International Strategy for Cyberspace; Department of Defense Strategy for Operating in Cyberspace; The National Military Strategy of the United States*; em 2013: *Department of Defense Cyberspace Workforce Strategy*; e em 2015: *National Security Strategy; The Department of Defense Cyber Strategy*; e *The National Military Strategy of the United States of 2015.*

Com o objetivo de analisar como os EUA incorporam o poder cibernético em seu poder militar, dos documentos supracitados serão investigados na sequência os dois referentes a segurança nacional elaborados pela Casa Branca (2010 e 2015) e os dois documentos elaborados pelo Departamento de Defesa (2011 e 2015). Pelas datas, observa-se que serão analisados os mesmos documentos contudo alguns referentes ao primeiro mandato de Obama, entre 2009 e 2012, enquanto outros sendo do segundo mandato, entre 2013 e 2016. Desse modo será possível realizar uma identificação mais aprofundada sobre a estratégia americana de incorporação do poder cibernético durante o governo Obama, com o levantamento comparativo de documentos destinados ao mesmo fim e a percepção de constâncias ou alterações nos direcionamentos de atuação no espaço cibernético.

4.2.1.1 As Estratégias de Segurança Nacional de 2010 e 2015 e o espaço cibernético

A National Strategy é um documento periodicamente reformulado pelo governo que contém os desafios à segurança do país e direcionamentos sobre como a administração planeja enfrentá-los.

Na National Security Strategy de 2009, o espaço cibernético entrou como uma questão de prioridade para a segurança nacional, com o entendimento de que ele é uma das ameaças mais sérias a segurança nacional, pública e econômica:

> *The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property* (THE WHITE HOUSE, 2010, p.27, grifo nosso).

Desse modo, o documento direciona a necessidade de construir-se novas estratégias para protegê-los dos ataques e desafios colocados pelas redes cibernéticas: "*In addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace*" (THE WHITE HOUSE, 2010, grifo nosso).

O Estado deixa clara sua vontade de fortalecer a segurança do espaço cibernético e de garantir que os militares tenham as capacidades de atuação em todos os domínios, incluindo o cibernético. No entanto, tratando-se das estratégias diretamente relacionadas a detenção, prevenção, detecção, defesa e recuperação do domínio após intrusões e ataques eles citam apenas duas estratégias. A primeira é voltada para investimento em pessoas e tecnologia propondo-se parceria com o setor privado para segurança tecnológica para proteger e aumentar a resiliência de infraestruturas críticas do governo e de empresas; investimento em pesquisa e inovação; e campanha nacional para promover a segurança cibernética.

A outra estratégia é direcionada a parcerias internacionais para buscar normas de conduta no meio, garantir a preservação, proteção, privacidade, livre circulação e acesso contínuo de dados além de discutir a realização da defesa e de respostas à ataques cibernéticos. Sobre os ataques cibernéticos, o documento acentua:

> *We will work with all the key players— including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents* (THE WHITE HOUSE, 2010, p. 28, grifo nosso).

Destaca-se a menção que o documento faz a parceria com aliados asiáticos, (Austrália, Filipinas, Tailândia e principalmente Japão e Coreia do Norte) para desenvolver uma agenda de segurança que junte esforços entre outros objetivos para a segurança cibernética.

Na *National Strategy* de 2015, os EUA continuaram vendo os desafios da segurança cibernética como sérios indo além ao enxergá-los como crescentes riscos associados à ataques cibernéticos de interrupção e destruição. Apesar disso, identificam avanços quanto às medidas que já tomaram: "*We are shaping global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats*" (THE WHITE HOUSE, 2015, p. ii, grifo nosso).

Logo a estratégia direciona a necessidade de fortalecer as infraestruturas do país "*against all hazards, especially cyber espionage and attack*" (THE WHITE HOUSE, 2015, p. 3, grifo nosso). As formas que o país buscou tornar mais seguro o espaço cibernético de acordo com a *National Strategy* de 2015 foi por meio de ação coletiva, a qual entre outros fins, deveria estar voltada também para a garantia de acesso aos espaços comuns, o cibernético, espacial, ar e oceanos.

Neste documento de 2015 a ênfase é maior na relação da defesa do espaço cibernético e exercício do poder militar. Em seção intitulada *Strengthen our National Defense* é clara essa relação através da evidente intenção do país em não só continuar investindo, mas em aumentar investimentos nas forças militares para que elas possam ter "*crucial capabilities like cyber*" (THE WHITE HOUSE, 2010, p. 3, grifo nosso).

Os Estados Unidos continuam dando relevância ao fato de que infraestruturas importantes do país possuem dependência do meio, como a economia, a saúde e que atores diversos como governos, grupos criminosos e atores individuais podem colocar sérios ataques. A estratégia para lidar com esses problemas continuou sendo em 2015 a de unir esforços do governo federal com o setor privado para fortalecer segurança e resiliência, assim como a continuidade de políticas de fomento a parcerias internacionais com foco em criar leis internacionais as quais possam impor custos aos atores maliciosos do espaço cibernético e proteger a propriedade intelectual, liberdade online e infraestruturas civis.

Um ponto de destaque sobre a segurança cibernética na *National Strategy* de 2015 não presente na de 2010 é a declaração a respeito da China: "*on cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government.*" (THE WHITE HOUSE, 2010, p. 3, grifo nosso). Os EUA deixaram clara a relação de adversidade no tema de segurança cibernética tratando-se da China.

Ambas as estratégias de segurança dos Estados Unidos do período Obama dão destaque à segurança cibernética, colocando o tema dentro do rol das ameaças prioritárias à segurança nacional, isto é, no patamar de ameaças como o terrorismo, mudanças climáticas e países adversários.

Os documentos levantam os riscos associados ao espaço cibernético como já tratados no capítulo anterior, ação de diversos atores, crimes cibernéticos (ameaça econômica e pública), além dos riscos à defesa nacional, ou seja, às infraestruturas críticas e aos sistemas governamentais e militares. No caso da defesa nacional, há a aproximação do tema com o poder militar, destacando-se o objetivo do país de garantir que as Forças tenham sempre capacidade de operar no domínio para impedir ataques, destruições e impedimentos de acesso e transmissão de dados.

Naturalmente, esses documentos não fazem nenhuma menção mais destacada sobre a atuação dos militares, porém trazem direcionamentos importantes para a segurança geral do país e são os documentos mais importante nacionalmente no tema, razão pela qual foram analisados aqui.

4.2.1.2 As Estratégias de Defesa Cibernética do Departamento de Defesa de 2011 e 2015

O Departamento de Defesa nos EUA é encarregado diretamente das questões de segurança nacional e das Forças Armadas. Nesse sentido é especialmente importante para o objetivo deste trabalho a análise dos documentos que o órgão elaborou porque eles conectam os objetos principais de estudo desta pesquisa, capacidades no espaço cibernético — poder cibernético —, defesa nacional desse espaço e Forças militares — poder militar.

Em 2011, o DoD lançou a *Strategy for operating in cyberspace* na qual delineou cinco iniciativas estratégicas para lidar com o novo contexto de ameaças imposto pelo espaço cibernético. Reconheceu a forte dependência que o órgão possui do meio virtual, naquele momento com quinze mil redes e sete milhões de computadores necessários para permitir operações militares, de inteligência, fornecimento de materiais e comando e controle das Forças, admitindo que diversos atores colocam riscos e buscam penetrar e interromper suas redes e sistemas.

Desse modo, de um lado o documento destacou as vulnerabilidades, trazendo a noção de que é preciso fortalecer o poder cibernético, isto é, a capacidade de atuar no meio e usá-lo estrategicamente para alcançar a defesa nacional. São evidenciadas como ameaças a facilidade de entrada no meio e de realização de ataques por diversos tipos de atores buscando explorar, interromper, negar e destruir informações, acessar propriedade intelectual provando como o meio cibernético realiza-se como um complexo desafio à segurança nacional.

Por outro lado, o documento também deu relevância as vantagens que o DoD possui no meio, a partir do poder que ele já exerce, como o profundo conhecimento que o órgão possui sobre a tecnologia de informação e comunicação, incluindo sua expertise em segurança cibernética além da habilidade do aparato militar do país em usar o espaço cibernético "*for rapid communication and information sharing in support of operations is a critical enabler of DoD missions*" (DEPARTMENT OF DEFENSE, 2011, p. 2, grifo nosso).

O foco do documento, contudo, é em apresentar as cinco iniciativas estratégicas do DoD para o espaço cibernético. A primeira iniciativa é de tratar esse meio como um domínio operacional para que sejam acessadas todas as vantagens que ele oferece. Essa estratégia está

correlacionada ao exposto na *National Security Strategy* de 2010 em que ficou declarada a necessidade de que as Forças possam operar em todos os domínios incluindo o cibernético. Para realização dessa iniciativa estratégica o Secretário de Defesa incubiu o *United States Strategic Command* (USSTRATCOM), os outros Comandos Combatentes e os departamentos militares de realizar missões no espaço cibernético.

Como já mencionado neste capítulo, o *U.S. Cyber Command*, criado para dar mais eficiência aos recursos e operações cibernéticas, foi colocado como uma subunidade do USSTRATCOM com o objetivo de sincronizar esforços de cada Força Militar: *U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, the 24th Air Force, U.S. Marine Corps Forces Cyber Command, and U.S. Coast Guard Cyber Command.* Até o início de 2018, o USCYBERCOM composto por 133 times esteve abaixo do USCYBERCOM, tendo em maio atingido completa autonomia operacional.

Ainda sobre esta iniciativa o documento ressalta que o "*DoD will fully integrate a complete spectrum of cyberspace scenarios into exercises and training to prepare U.S. Armed Forces for a wide variety of contingencies*" (DEPARTMENT OF DEFENSE, p. 6, grifo nosso). Com isso, ele demonstra a preocupação de que ações no espaço cibernético afetem outros domínios, o que corrobora com o expressado no capítulo dois, quando definido o poder cibernético e levantada a discussão de que é característico a propriedade de estender-se para outros poderes e domínios. Nessa primeira iniciativa já está clara a incorporação do poder cibernético ao militar por meio da preparação das Forças para operar no meio virtual.

A segunda iniciativa estratégica do documento defende que o DoD adotará conceitos novos de operação de defesa para proteger redes e sistemas, acreditando que esse é um passo necessário para garantir a segurança cibernética especialmente ao longo dos anos e aprimoramento tecnológico. Desse modo, o órgão propôs-se a melhorar o monitoramento e a comunicação interna, a empregar uma defesa ativa e a desenvolver novos conceitos de defesa e meios nos dispositivos de informática.

A terceira iniciativa estratégica encontrando mais uma vez com princípios expostos na National Security Strategy de 2010 trata das parcerias do DoD tanto com outras agências e departamentos do governo dos EUA como o DHS, quanto com o setor privado para apoiar o desenvolvimento conjunto de medidas de segurança e defesa cibernéticas. A quarta iniciativa

também é voltada ao projeto de parcerias, no entanto, nesse caso internacionais com o objetivo de garantir a liberdade, a privacidade e a circulação de informação. Para a realização dessa estratégia, o DoD prevê o uso das Forças militares com a finalidade de promover a defesa coletiva dos EUA e dos países aliados, além de aumentar as possibilidades de dissuasão coletiva no espaço cibernético: "*DoD will expand its formal and informal cyber cooperation to a wider pool of allied and partner militaries to develop collective self-defense and increase collective deterrence*" (DEPARTMENT OF DEFENSE, 2011, p. 10, grifo nosso).

A última iniciativa estratégica prevista nesse documento é para aumentar a perspicácia do país através do estabelecimento de uma excelente força cibernética e da rápida inovação tecnológica, atendendo mais uma vez ao expresso na NSS de 2010, quanto aos investimentos voltados para a inovação e enfrentamento dos desafios. Especialmente importante sobre essa estratégia é a centralidade e a relevância que o documento apresenta para a formação da força cibernética, reforçando a necessidade de serem selecionadas, e treinadas pessoas de alto talento, com a organização de uma Guarda Nacional e de Reserva com capacidades cibernéticas para investir o DoD com maior expertise e flexibilidade de atuação.

Sendo assim, por meio desse documento o DoD reconheceu as mudanças para a segurança nacional que o espaço cibernético implica e direcionou as oportunidades e modos de operacionalizar o poder cibernético com o poder militar. Isso é claro na primeira, quarta e quinta iniciativas, em que respectivamente o Departamento afirma que esse meio virtual é um domínio que deve ser integrado nas atuações das Forças militares; coloca o objetivo do Estado em promover a cooperação internacional militar para garantir a defesa cibernética coletiva; e centraliza a importância de ser organizada uma Força nacional para atuação no espaço cibernético. De modo geral, a 2011 DoD *Strategy for Operating in Cyberspace* fez poucas referências às capacidades cibernéticas operacionais e ofensivas dos EUA, diferentemente do documento posterior como apresentado a seguir.

Em 2015 o Departamento de Defesa dos EUA lançou a segunda segunda estratégia para o espaço cibernético contendo também cinco objetivos estratégicos, os quais voltaram-se "*from workforce and human capital development to full integration of cyber capabilities into military operations and deterrence*" (ZHENG, 2015, grifo nosso).

Essa estratégia foi publicada no ano seguinte ao ataque cibernético sofrido pela Sony considerado pelo próprio DoD no documento como o maior caso sofrido por uma entidade americana. Nesse evento a Coreia do Norte roubou cópias digitais de vários filmes que ainda não haviam sido lançados, além de documentos com informações sobre celebridades, empregados e informações administrativas da Sony.

O primeiro ponto importante dessa estratégia são as *Three Primary Missions in Cyberspace* do Departamento de Defesa americano. Notando que "the increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations" (DEPARTMENT OF DEFENSE, 2015, p. 2), o DoD encarregou-se de três missões cibernéticas primárias, que associam intimamente o poder cibernético ao militar para a ocorrência da defesa nacional: i) defender suas redes, sistemas e informações; ii) defender os EUA e seus interesses contra ataques cibernéticos de consequência significante, isto é, ataques que possam provocar "*loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States*" (DEPARTMENT OF DEFENSE, 2015, p. 5, grifo nosso); iii) prover quando necessário capacidades cibernéticas para apoiar operações militares e planos de contingência em casos entendidos como apropriados aos Estados Unidos conduzirem operações "*to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations*" (DEPARTMENT OF DEFENSE, 2015, p. 5, grifo nosso)

Outro ponto importante trazido no documento foi a divulgação da Cyber Mission Force, um investimento iniciado em 2012 que segundo o documento quando estivesse operacionalizando integralmente contaria com "*nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components [...] organized into 133 teams*" (DEPARTMENT OF DEFENSE, 2015, p. 6, grifo nosso). Esse foi um avanço relevante no aprofundamento do poder cibernético estratégico do país e desde 2013 o Departamento buscou integrar a CMF "*into the larger multi mission U.S. military force to achieve synergy across domains, assure the CMF's readiness within the force[...]*" (DEPARTMENT OF DEFENSE, 2015, p. 7, grifo nosso), um claro avanço no sentido de incorporar o poder cibernético ao militar.

Nota-se diante do exposto, que o poder cibernético desenvolvido nos EUA recebe esforços para que incorporado ao poder militar entre em sinergia com as demais Forças militares. No entanto, com a própria criação do CMF o país incorpora o poder cibernético ao seu poder nacional, no rol do poder militar dentro do DoD sem necessariamente associá-lo às forças convencionais. Esse fato confirma parcialmente a hipótese do trabalho que levanta a possibilidade de que o poder cibernético é incorporado associado às demais forças nos EUA, ficando claro aqui que não diretamente, nem primariamente.

Seguindo na análise dos pontos trazidos na Cyber Strategy de 2015 percebe-se outro ponto muito relevante aqui que são as cinco metas estratégicas para que o DoD possa realizar as suas três missões primárias no espaço cibernético citadas anteriormente, por isso mesmo em alguns aspectos muito semelhantes a elas. Primeiramente, construir e manter forças e capacidades para operar no espaço cibernético. Em segundo lugar, defender as redes de informação, dados e mitigar riscos às missões do DoD. Em terceiro lugar, defender os EUA e seus interesses de ataques com consequências significativas. Em quarto lugar, construir e manter viável opções cibernéticas como seu uso planejado para controlar a escalada de conflitos e definir o ambiente de conflito. Em último lugar, aumentar alianças e parcerias internacionais para construir e manter a segurança e a estabilidade.

Percebe-se nas estratégias do DoD esforços em colocar o espaço cibernético como um domínio, vinculá-lo ao poder militar para superar as vulnerabilidades do país e em investir em pessoas capacitadas e aprimoramento das tecnologias para garantir a defesa cibernética.

4.3 CONCLUSÕES PARCIAIS

O poder cibernético entendido como capacidade de atuar no espaço cibernético esteve desde a criação desse meio intrinsecamente relacionado ao poder militar. O processo de aprofundamento dessa associação ocorre no período Obama quando o tema ganha maior visibilidade em documentos oficiais.

A mobilização da força aérea para criar capacidades cibernéticas iniciou o movimento de segurança e defesa nacional nos EUA, mas foi com Obama que as forças militares passaram a desenvolver suas estruturas próprias de defesa e também realizaram esforços conjuntos através do USCYBERCOM.

Conforme aprofundou-se no país a percepção dos riscos que os crescentes ataques a suas redes e sistemas implicam, diversos documentos totalmente ou parcialmente voltados para o tema segurança e defesa cibernética foram lançados buscando colocar o modo estratégico como o país trataria as novas questões do espaço cibernético. Na análise das NSS de 2010 e de 2015 e das estratégia cibernéticas do DoD de 2011 e de 2015, observou-se os esforços do país em tratar o espaço cibernético como uma questão de prioridade, elevá-lo ao posto de domínio e criar e aprimorar as condições do país para exercer poder nesse meio.

5 CONCLUSÃO

O poder permeia toda ação política internacional, sendo imprescindível para que os Estados atinjam seus interesses e garantiamr sua sobrevivência no meio anárquico. O contexto moldado por alterações estruturais ou pelos objetivos realistas da nação em conservar, aumentar ou demonstrar poder tem a capacidade de alterar o tipo de poder buscado, o conteúdo e a maneira de empregá-lo.

Como a política dos Estados é perpassada pelo poder como um fim em si mesmo ou como meio para atingir outros objetivos, afirma-se que a política internacional é uma luta pelo poder, que frequentemente toma a forma de uso da força ou ameaça de seu uso, sendo, desse modo, a efetivação do poder militar, um dos três tipos de poder nacional — econômico, diplomático e militar.

O poder se relaciona com a capacidade de controlar e determinar resultados tanto quanto maior for a potencialidade de o país articular e aprofundar seus poderes nacionais. Tratando-se da defesa do Estado, destaca-se o poder militar, isto é, o controle sobre todos os domínios que apresentam ameaças aos países.

O exercício do poder militar permite ao Estado, pelo uso legítimo da força e de sua ameaça, tanto a garantia de sua sobrevivência e segurança estatal, quanto o alcance de seus objetivos políticos. Utilizando-se do poder marítimo, terrestre e aéreo pertencentes ao espectro do poder militar, por muito tempo foi suficiente aos Estados atingirem seus interesses e manter a segurança nacional. As transformações no mundo, contudo, trazem novos desafios aos Estados.

A emergência do espaço cibernético e dos riscos associados a ele demonstram que, se um país quiser deter poder internacional, garantir sua sobrevivência, segurança e interesses, necessariamente precisa desenvolver capacidades de operacionalizar nesse novo meio, o que só é possível via poder cibernético.

Nesse contexto, os Estados são impulsionados a buscar o poder cibernético temendo um desequilíbrio de poder internacional e a ocorrência de uma possível guerra. Vendo-se ameaçados pelo espaço cibernético devido às várias características do meio que evidenciam suas vulnerabilidades — anarquia, facilidade de entrada e de atuação, anonimato —, e pela ocorrência de ataques cibernéticos, os quais quando de maior impacto são perpetrados por

atores estatais, os países atentam-se mais sobre as questões de insegurança cibernética internacional e para o desbalanceamento de poder cibernético internacional.

Buscando vencer não só os riscos do espaço cibernético, mas também acessar as vantagens desse meio, os Estados vão buscar desenvolver o poder cibernético atrelando-o à sua estratégia de segurança e defesa nacional.

Este trabalho, portanto, preocupou-se especificamente em entender como os Estados Unidos estão incorporando o poder cibernético ao militar, tendo como recorte temporário o governo Obama.

Observando-se os documentos da NSS de 2010 e 2015 e as estratégias para o espaço cibernético do DoD de 2011 e de 2015, concluiu-se que o espaço cibernético é uma questão de prioridade para a segurança nacional, entendido como um domínio sobre o qual o país deve e efetivamente está investindo em pessoas, tecnologia e parcerias para promover a segurança e a defesa cibernéticas contra seus adversários, especialmente Estados, os quais podem exercer um impacto maior mediante um ataque cibernético.

A hipótese levantada de que a incorporação do poder cibernético ao militar ocorre de modo complementar às estratégias militares convencionais, unicamente associado às demais Forças não se confirmou. Percebem-se esforços dos EUA em transformar o espaço cibernético em um domínio, em garantir que as Forças militares convencionais tenham capacidade de atuação também nele, a criação do USCYBERCOM que reúne esforços de cada Força, contudo nota-se pela leitura dos documentos, que, embora interligada aos demais poderes militares, a estratégia de desenvolvimento de poder cibernético não é pensada com o objetivo único de complementar os poderes militares convencionais, tampouco essa estratégia de incorporação do poder cibernético é articulada necessariamente associada às outras Forças.

O próprio ato de desenvolver uma estratégia específica para o meio cibernético já demonstra o caráter individual e independente desse domínio, que, por isso, recebe um tratamento individual e independente em relação a outros tipos de poderes militares.

Entra na estratégia do país a concepção de que o espaço cibernético também servirá aos engajamentos militares das demais Forças e que elas devem ter meios para atuar quando necessário, e que o USCYBERCOM pode apoiar operações contra inimigos fazendo um primeiro ataque, por exemplo, desestabilizando redes essenciais para os adversários. No

entanto, a estratégia estadunidense para tratar a segurança e a defesa do espaço cibernético não é pensada voltada exclusivamente para os demais poderes militares.

Há o entendimento militar, nos EUA, de que o espaço cibernético é um domínio que pode impactar os demais, bem como e outros poderes, o que coloca a necessidade de muitas vezes associar o poder cibernético aos demais. Contudo, há uma preponderância nos documentos para a visão de que, como um domínio independente, requer investimentos exclusivos e uma Força também exclusiva, razão pela qual o país criou a Cyber National Mission Force. Logo o poder cibernético vem sendo, nos últimos anos, desenvolvido de modo independente em relação às demais Forças nos Estados Unidos.

A Cyber National Mission Force conduz operações no espaço cibernético para impedir e negar ataques adversários contra sistemas e infraestruturas críticas da nação: "*it is the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations*" (CROWTHER, 2018, grifo nosso). Essa força é resultado de um processo iniciado ainda em 2013 porém completamente operacionalizado e funcional apenas em 2018: "t*he cyber mission force has been building capability and capacity since 2013, when the force structure was developed and the services began to field and train the force of over 6,200 soldiers, sailors, airmen, Marines and civilians*" (DOD, 2018).

Importante aqui deixar claro que neste trabalho defende-se que o poder cibernético existe de modo independente em relação às demais Forças na estratégia estadunidense, mesmo observando que o USCYBERCOM é composto por unidades de cada uma das Forças e que, além disso, a Cyber Mission Force é composta majoritariamente por militares. Tais realidades não modificam o fato de que o espaço cibernético seja pensado também de modo desvinculado dos demais domínios e expressões do poder militar. Por ser um espaço com características próprias e desafios únicos, a forma de efetivar a estratégia para ele não pode e de fato não é pensada unicamente vinculada aos demais poderes.

Além do mais, em maio de 2018 o USCYBERCOM foi tornado autônomo em relação ao USSTRATCOM. Esse novo direcionamento da estratégia estadunidense para o espaço cibernético mostram que provavelmente no futuro a defesa cibernética estará ainda menos atrelada às forças convencionais. O estabelecimento da *Cyber National Mission Force* foi entendida pelo DOD como a colocação de um exército cibernético: "*the cyber mission force is*

Cybercom's action arm, and its teams execute the command's mission to direct, synchronize and coordinate cyberspace operations in defense of the nation's interests" (DOD, 2018).

Tal fato sugere que, nos próximos anos, a necessidade de especialidade em desenvolver a Defesa Cibernética seja tamanha que uma força única, destinada exclusivamente para pensar as ações no domínio cibernético seja o caminho a ser seguido pelas demais nações. Se, atualmente, a força cibernética é composta por militares das demais forças, talvez isso não seja verdade no futuro.

Com a dissociação do USCYBERCOM do STRATCOM e criação da *Cyber National Mission Force*, treinada há alguns anos, os EUA parecem temer uma intensificação das ameaças atreladas ao espaço cibernético. Como mostrado neste trabalho, há fortes razões para que os Estados desenvolvam o poder cibernético e o destinem à defesa nacional. É evidente o aprofundamento da dependência virtual e o rápido desenvolvimento da tecnologia. Acreditar na possibilidade de conflitos maiores e mais destrutivos nesse domínio dentro de poucos anos não é uma ficção e as medidas de segurança dos EUA afirmam tal concepção. Ampliar o poder de defesa do Estado pela incorporação do poder cibernético ao militar é uma necessidade cada vez mais real.

Sendo assim, conclui-se que o poder cibernético é incorporado ao poder militar no sentido de complementar as estratégias militares convencionais, no entanto não possui essa única finalidade, visto que os documentos militados analisados aqui tratam o espaço cibernético como um domínio independente dos demais, requerendo suas próprias capacidades de defesa e não tendo o propósito único de servir a outros domínios. Logo, o poder cibernético é abordado pela estratégia americana como podendo, sim, ser efetivado de modo independente das demais Forças, sendo inclusive construído cada vez mais no sentido de ocupar patamares equiparados aos poderes aéreo, marinho, terrestre e, mais recentemente, espacial.

REFERÊNCIAS

AMARAL, Arthur. **A guerra ao terror e a tríplice fronteira na agenda de segurança dos Estados Unidos.** Dissertação, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008.

ARQUILLA, John, and RONFELDT, David. **The Advent of Netwar**. Santa Monica: Rand Corporation, 1996.

BALDWIN, David A. **Power and International Relations:** a conceptual approach. New Jersey: Princeton University Press, 2016.

BARLOW, John Perry. **A declaration of the independence of cyberspace.** EFF: Davos, 1996. Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em: 20 out. 2018.

BARNARD-WILLS, David; ASHENDEN, Debi. **Securing virtual space: cyber war, cyber terror, and risk. Space and culure.** Swindon, Cranfield University, v. 15, ed. 2, p. 110-123, 2012. Disponível em: <http://journals.sagepub.com/doi/abs/10.1177/1206331211430016>. Acesso em: 24 set. 2018.

BENDRATH, Ralf. **The cyberwar debate:** Perception and politics in U.S. critical infrastructure protection. Information & Security, vol 7, 2001, p. 80-103.

BERNART JUNIOR, Stefan Cavalcante. **O Setor Cibernético nos Estados Unidos da América:** ensinamentos para o Exército Brasileiro.Trabalho de Conclusão de Curso (Especialização) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

BERWANGER, Tiago. **O discurso de securitização da cibernética nos Estados Unidos da América no período entre 2007 e 2015.** Monografia de graduação, Florianópolis, UFSC, 2015.

BULL, Hedley. **A sociedade anárquica.** Brasília, Ed. da UnB/ IPRI, 2002.

CARNEIRO, João Marinonio Enke. **A guerra cibernética:** uma proposta de elementos para a formulação doutrinária no Exército Brasileiro. Tese - Escola de Comando e Estado-Maior do Exército, 203f, Rio de Janeiro, 2012.

CARR, Edward. **Vinte anos de crise 1919–1939.** Brasília: Editora UnB, 2001.

CASTRO, Thales. **Teoria das relações internacionais.** Brasília: FUNAG, 2012.

CASTRO, Therezinha. **Geopolítica:** princípios, meios e fins. Rio de Janeiro: Bibliex, 1999.

CHIAPPIN, José R. N. **Os fundamentos teóricos do programa do realismo em política internacional:** a concepção de Morgenthau e epistemologia da política de poder. Carta Internacional, v. 4, n. 2, 2010. Disponível em: <https://cartainternacional.abri.org.br/Carta/article/view/523>. Acesso em: 19 out. 2018.

CLARKE, Richard A.; KNAKE, Robert K. **Cyberwar:** the next threat to national security and what to do about it. Harper Collins. EPub Edition, 2010.

CLAUSEWITZ, Carl von. **Da Guerra**. São Paulo: Martins Fontes, 2003.

CLAYTON, Mark. A year of Stuxnet: Why is the new cyberweapon's warning being ignored? **The Christian Science Monitor**. 26 out. 2011. Disponível em:

<https://www.csmonitor.com/USA/2011/0926/A-year-of-Stuxnet-Why-is-the-new-cyberweapon-s-warning-being-ignored>. Acesso em 07 out. 2018

CROWTHER, Alexander G. National Defense and the cyber domain. In: THE HERITAGE FOUNDATION. **2018 Index of U.S. military strength.** Washington, D.C.: The Heritage Foudation, 2018. Disponível em: <https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf>. Acesso em: 31 ago. 2018.

CSIS — CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. **From awareness to action:** a cybersecurity agenda for the 45th President. Washigtion, D.C.: CSIS, 2017. Disponível em: <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf>. Acesso em 07 out. 2018

CSIS; UNIDIR. **Report of the International Security cyber issues workshop series.** 2016. Disponível em:<https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity-4>. Acesso em: 09 out. 2018

DAHL, Robert. The concept of power. **Behavioral Science**, nº 2, v. 3, jul. 1957.

DEPARTMENT OF DEFENSE. **Department of Defense Strategy for Operating in Cyberspace.** July 2011. Disponível em: <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>. Acesso em: 17 out. 2018.

DEPARTMENT OF DEFENSE. **The Department of Defense Cyber Strategy.** April 2015. Disponível em: <http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf>. Acesso em: 17 out. 2018.

DEPARTMENT OF DEFENSE. **Cyber Mission Force Achieves Full Operational Capability.** May 17, 2018. Disponível em: <https://dod.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/>. Acesso em: 17 out. 2018.

DODGE, Michaela; INSERRA, David R. Strategic capabilities in the 21st century. In: WOOD, Dakota L. **2015 Index of U.S. Military strength:** assessing America's ability to provide for the common defense. Washington, D.C: The Heritage Foundation, 2015.

ESTADOS UNIDOS DA AMÉRICA. Department of the Army. **Cyberspace operations concept capability plan 2016-2028.** Washigton, D.C: Department of the Army, 2010. Disponível em: <https://fas.org/irp/doddir/army/pam525-7-8.pdf>. Acesso em: 31 ago. 2018.

FERREIRA NETO, Walfredo Bento. **Por uma geopolítica cibernética:** apontamentos da grande estratégia brasileira para uma nova dimensão da guerra. Dissertação Universidade Federal Fluminense, Niterói, 2013, 212f.

FRAZÃO, Pedro Henrique Oliveira. **Um big brother global?** Os programas de vigilância da NSA à luz da securitização dos espaços sociotecnológicos. Dissertação (Programa de Pós-Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2016, 130p.

GADY, Franz-Stefan; AUSTIN, Greg. **Russia, The United States, and Cyber Diplomacy:** Opening the doors.EastWest Institute, 2010. Disponível em: <https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf>. Acesso em: 10 out. 2018.

GOMEZ, Miguel Alberto N. **Arming cyberspace:** the militarization of a virtual domain. Global Security and Intelligence Studies, v.1, nº 2, 2016. Disponível em:<http://digitalcommons.apus.edu/gsis/vol1/iss2/>. Acesso em: 24 set. 2018.

GRAÇA, Pedro José Bentes. **O Ciberataque como Guerra de Guerrilha:** o caso dos ataques DoS/DDoS à Estônia, Geórgia e ao Google-China. Universidade de Lisboa, Instituto Superior de Ciências Sociais e Políticas, Dissertação, Lisboa, 2013. Disponível em: <https://www.repository.utl.pt/bitstream/10400.5/8000/1/Tese.pdf>. Acesso em: 09 out. 2018.

HERZ, John. **Idealist internationalism and the security dilemma.** World Politics, vol.2, nº 2, jan. 1950.

HJALMARSSON, Ola. **The securitization of cyberspace.** Lund University, Department of Political Science, 2013. Disponível: <https://lup.lub.lu.se/student-papers/search/publication/3357990>. Acesso em: 16 out. 2018.

HOBBES, Thomas. **Leviatã:** Matéria, forma e poder de um Estado eclesiástico e civil. Tradução de João Paulo Monteiro e Maria Beatriz Nizza da Silva. 3. ed. São Paulo: AbrilCultural, 1983. (Os Pensadores).

KRAMER, Franklin. Cyberpower and National Security: policy recommendations for a strategic framework. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry. **Cyberpower and National Security.** Washington, D.C.: NDU Press, 2009.

KUEHL, Daniel T. From cyberspace to cyberpower: defining the problem. In: KRAMER, Franklin D.; STARR, Stuart; WENTZ, Larry K. **Cyberpower and National Security.** Washington, D.C.: NDU Press, 2009, p1-17. Disponível em: <https://www.jstor.org/stable/j.ctt1djmhj1>. Acesso em: 03 set. 2018.

LACHOW, Irving. Cyber Terrorism: Menace or Myth? In: KRAMER, Franklin D.; STARR, Stuart; WENTZ, Larry. **Cyberpower and National Security.** Washington, D.C.: NDU Press, 2009.

LIBICKI, Martin C. **Conquest in cyberspace:** National Security and Information Warfare. California: Cambridge University Press, 2007.

MAC ISAAC, David. Vozes do azul: teóricos do poder aéreo. In: Peter Paret (Org.). **Construtores da Estratégia Moderna**. Tomo 2. Rio de Janeiro: Biblioteca do Exército Editora. 2001. p. 211-242.

MANJIKIAN Mary McEvoy. From global village to virtual battlespace: The colonizing of the Internet and the extension of realpolitik. **International Studies Quarterly**, n. 54, p. 381 – 401, 2010.

MELLO, Leonel. **A geopolítica do poder terrestre revisitada.** Lua Nova, São Paulo , n. 34, p. 55-69, dez. 1994. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-64451994000300005&lng=en&nrm=iso>. Acesso em: 09 out. 2018.

MINGST, Karen. **Princípios de relações internacionais.** Rio de Janeiro: Elsevier, 2009.

MORGENTHAU, Hans. **A política entre as nações:** a luta pelo poder e pela paz. Brasília: Editora UnB, IOESP, IPRI, 2003.

NATIONAL SECURITY COUNCIL. (2010). **The comprehensive national cybersecurity initiative.** 2010. Disponível em: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>. Acesso em: 20 out. 2018

NYE, Joseph. **Cyber power**. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.

OBAMA, Barack. **President Obama's Remarks on Securing U.S. Cyber Infrastructure**. Washigton, D.C.: The White House, 2009. Disponível em: <http://www.america.gov/st/texttrans-english/2009/May/20090529161700eaifas0.1335871.html>. Acesso em: 10 out. 2018.

PERON, Alcides Eduardo dos Reis. Guerra virtual e eliminação da fricção? O uso da cibernética em operações de contrainsurgência pelos EUA. In: OLIVEIRA, Marcos Aurélio Guedes de; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar. **Relações Internacionais Cibernéticas (CiberRI):** oportunidades e desafios para os estudos estratégicos e de segurança internacional.Recife: Editora UFPE, 2016.

RATTRAY, G.; Evans, C.; HEALY, J. American security in the cyber commons. In: DENMARK, A. M.; MULVENAN, J. **Contested commons**: The future of American power in a multi-polar world. Washington, DC: Center for a New American Security, 2010, p.137-176.

REINO, Lucas. **Antes da internet - as ideias que embasaram a criação da rede mundial de computadores.** In: 10º Encontro Nacional de História da Mídia - Alcar, 2015, UFRGS, Porto Alegre, RS. Disponível: http://www.ufrgs.br/alcar/encontros-nacionais-1/encontros-nacionais/10o-encontro-2015/historia-da-midia-digital/antes-da-internet-2013-as-ideias-que-embasaram-a-criacao-da-rede-mundial-de-computadores/view. Acesso em 30 set. 2018.

RITUERTO, Ricardo Martínez. **Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE.** El País, Bruxelas, 18 maio 2007. Disponível em:<https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html>. Acesso em: 09 out. 2018.

SCHNEIER, Bruce. **The story behind the Stuxnet virus.** Forbes, 2010. Disponível em: <https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.htm>. Acesso em: 09 out. 2018.

SEWALL, Sarah et al. **The US Army / Marine Corps Counterinsurgency Field Manual**. Chicago: University of Chicago Press, 2007.

SHELDON, John B. Deciphering cyberpower: strategic purpose in peace and war. **Strategic Studies Quaterly**, p. 95-112, 2011.

_____. The rise of cyberpower. In: BAYLIS, John; Wirtz, James J; GRAY, Colin S. **Strategy in the contemporary world: an introduction to Strategic Studies.** Oxford University Press, 2015.

SHIMKO, Keith L. The United States and the RMA: revolutions do not revolutionize everything. COLLINS, Jeffrey; FUTTER, Andrew. **Reassessing the revolution in military affairs:** transformation, evolution and lessons learnt. Nova York: Palgrave Macmillan, 2985.

MCNAB, Chris; WIEST, Andrew. **A história da guerra do Vietnã.** São Paulo: M.books, 2016.

SOUZA, Gills Lopes Macêdo. **Reflexos da digitalização da guerra na política internacional do século XXI:** uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. Dissertação (mestrado). Universidade Federal de Pernambuco, CFCH. Programa de Pós-Graduação em Ciência Política, Recife, 2013.

THE WHITE HOUSE. **National Security Strategy.** Washington, maio de 2010. Disponível: <http://nssarchive.us/NSSR/2010.pdf>. Acesso em: 16 out. 2018.

_____. **National Security Strategy.** Washington, maio de 2015. Disponível: <http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf. Acesso em: 16 out. 2018.

UNIDIR. **The Cyber Index:** International Security Trends and Realities. United Nations Publications, 2013. Disponível em: <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>. Acesso em: 08 out.18

UIT. **Global Cybersecurity Index (GCI) 2017.** Disponível em:<https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf>. Acesso em: 07 out. 2018

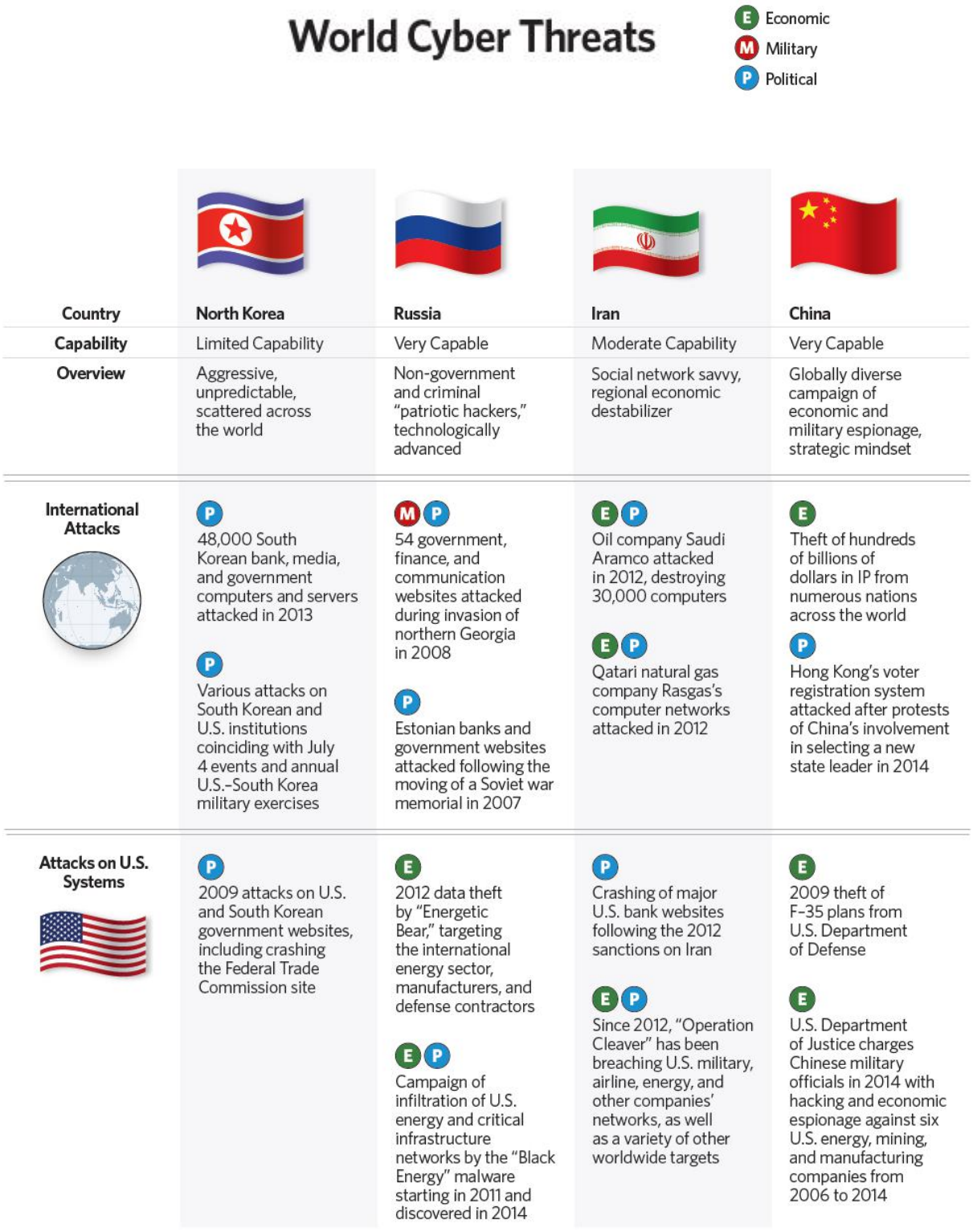
WALTZ, Kenneth. **O homem, o estado e a guerra:** uma análise teórica. São Paulo: Martins Fontes, 2004,.

_____. **Theory of International Politics.** Reading, Mass.: Addison-Wesley,1983.

WIGHT, Martin. **A política do poder.** Brasília: Editora UnB, IPRI; São Paulo: IOESP, 2002.

ZHENG, Denise E. **2015 DOD Cyber Strategy.** Center for Strategic and International Studies, 2015. Disponível em: <https://www.csis.org/analysis/2015-dod-cyber-strategy>. Acesso em: 18 out. 2018.

ANEXO A — *2015 Index of US Military Strenght*



Fonte: Heritage Foundation, 2015, p. 78.